MODELLO DI ORGANIZZAZIONE, GESTIONE e CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001 n. 231

Approvato in data 14 Giugno 2019

Porto di Trieste Servizi S.r.l.
Via Karl Von Bruk, 3
34122 Trieste (Italy)

C.F/P.I.: 01159270329
Iscr. Reg. Imprese n. TYS - 129117

Sommario

PARTE GENERALE 6

DEFINIZIONI 7

PREMESSA 9

PARTE PRIMA 10

IL DECRETO LEGISLATIVO 231/2001 10

SOGGETTI, FATTISPECIE CRIMINOSE E SANZIONI 10

1.1. La Responsabilità amministrativa degli enti 10

1.2. Definizione di rischio accettabile e fattispecie criminose 11

1.3. La condizione esimente della responsabilità amministrativa dell'Ente 14

1.4. Le Linee guida di Confindustria 15

PARTE SECONDA 17

IL MODELLO ORGANIZZATIVO DI PORTO DI TRIESTE SERVIZI S.r.l. 17

2.1. Elementi fondamentali del Modello 17

2.2. Modello, Codice Etico e sistema disciplinare 17

2.3. Politica integrata con il Sistema di Gestione della Qualità (SGR) 18

PARTE TERZA 20

PORTO DI TRIESTE SERVIZI S.r.l. 20

3.1. La storia e lo sviluppo della Società 20

3.2. Governance 22

3.3. Organigramma 24

PARTE QUARTA 25

LA COSTRUZIONE DEL MODELLO 25

4.1. Struttura del Modello 25

4.2. Principi di controllo nelle potenziali aree di attività a rischio 26

4.3. Misurazioni, analisi e miglioramenti 28

PARTE QUINTA 29

L'ORGANISMO DI VIGILANZA 29

5.1. I requisiti 29

5.2. Individuazione 29

5.3. Nomina 30

5.4. Funzioni 30

5.5. Flussi informativi 32
PARTE SESTA 34
INFORMAZIONE E FORMAZIONE 34
6.1. Informazione, formazione ed aggiornamento 34
PARTE SETTIMA 35
DESTINATARI E CAMPO DI APPLICAZIONE 35
PARTE OTTAVA 36
PROCEDURA DI ADOZIONE DEL MODELLO 36
PARTE NONA 37
IL SISTEMA DISCIPLINARE 37
9.1. Principi generali 37
9.2. Sanzioni per i lavoratori subordinati cui si applicano i Contratti Collettivi Nazionali di Lavoro 37
9.3. Misure nei confronti dei dirigenti 38
9.4. Misure nei confronti degli Amministratori 38
9.5. Misure nei confronti dei Sindaci 38
9.6. Misure nei confronti dell'Organismo di Vigilanza 38
9.7. Misure nei confronti di Consulenti e Partner/Fornitori 39
PARTE DECIMA 40
GESTIONE DELLE SEGNALAZIONI -WHISTLEBLOWING (L. 30.11.2017 n. 179) 40
10.1. Premessa 40
10.2. Il ruolo dell'Organismo di Vigilanza 40
10.3. Nullità delle misure ritorsive e discriminatorie adottate nei confronti del segnalante. 41
10.4. Perdita delle tutele garantite dalla legge in caso di malafede del segnalante 42
PARTE SPECIALE 43
PARTE UNDICESIMA 44
FINALITÁ E STRUTTURA DELLA PARTE SPECIALE 44
11.1. Finalità della Parte Speciale 44
11.2. Struttura della Parte Speciale 45
11.3. Principi ispiratori 46
11.4. Il sistema dei poteri e delle deleghe 46
PARTE DODICESIMA 48
ANALISI E MAPPA DEI RISCHI 48
12.1. Premessa 48
12.2. Metodologia di lavoro 48
12.3. Individuazione dei processi aziendali di interesse ai fini del D. L.gs. 231/2001 48

12.4. Mappa dei rischi “231” e valutazione 50
12.5. Specifiche circa i delitti tentati 51
12.6. Considerazioni finali 51
PARTE TREDICESIMA 53
REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE 53
13.1. Criteri per la definizione di P.A. e di soggetti incaricati di un pubblico servizio 53
13.2. Enti della Pubblica Amministrazione 53
13.3. Pubblici Ufficiali 54
13.4. Incaricati di Pubblico Servizio 55
13.5. Le Società in house nella prospettiva del D. L.gs. 231/2001 56
13.6. Le fattispecie di reato richiamate dal D. L.gs. 231/2001 58
13.7. Attività sensibili relative ai reati contro la Pubblica Amministrazione 62
13.7. Organi e funzioni aziendali coinvolte 63
13.8. Principi e regole generali di comportamento 65
13.9. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 68
13.10. I controlli dell’Organismo di Vigilanza 69
PARTE QUATTORDICESIMA 70
REATI SOCIETARI 70
14.1. Le fattispecie di reato richiamate dal D. L.gs 231/2001 70
14.2. Le attività sensibili relative ai reati societari 74
14.3. Organi e funzioni aziendali coinvolte 75
14.4. Principi e regole generali di comportamento 75
14.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 77
14.6. I controlli dell’Organismo di Vigilanza 81
PARTE QUINDICESIMA 83
REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI 83
15.1. Le fattispecie di reato richiamate dal D. L.gs. 231/2001 83
15.2. Le attività sensibili relative ai reati informatici 89
15.3. Organi e funzioni aziendali coinvolte 90
15.4. Principi e regole generali di comportamento 90
15.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 92
15.6. I controlli dell’Organismo di Vigilanza 94
PARTE SEDICESIMA 96
REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI O UTILITÁ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO 96

16.1. Le fattispecie di reato richiamate dal D. L.gs. 231/2001 96
16.2. Le attività sensibili relative ai reati di ricettazione, riciclaggio ed impiego di denaro, bene o utilità di provenienza illecita, nonché autoriciclaggio 98
16.3. Organi e funzioni aziendali coinvolte 99
16.4. Principi e regole generali di comportamento 99
16.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 99
16.6. I controlli dell'Organismo di Vigilanza 100
PARTE DICIASETTESIMA 102
REATI AMBIENTALI 102
17.1. Le fattispecie di reato richiamate dal D. L.gs. 231/2001 102
17.2. Le attività sensibili relative ai reati ambientali 103
17.3. Organi e funzioni aziendali coinvolte 103
17.4. Principi e regole generali di comportamento 104
17.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 104
17.6. I controlli dell'Organismo di Vigilanza 104

PARTE GENERALE

DEFINIZIONI

DESTINATARI

Componenti degli Organi sociali, coloro che svolgono funzioni di gestione, amministrazione, direzione o controllo della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, i dirigenti, i dipendenti della Società ed in generale quanti si trovino ad operare sotto la direzione e/o vigilanza delle persone suindicate.

PERSONALE

I dipendenti ed i collaboratori che prestano la loro opera a favore di PTS in forme contrattuali anche diverse da quella del lavoro subordinato.

CCNL

Contratti Collettivi Nazionali di Lavoro attualmente in vigore ed applicati dalla Società.

CONSULENTI

Coloro che agiscono in nome e/o per conto di PTS sulla base di incarichi di consulenza.

D. L.GS. 231/2001 O DECRETO

il decreto legislativo n. 231/2001 e successive modifiche.

PTS, LA SOCIETÀ O L'AZIENDA

Porto di Trieste Servizi S.r.l.

AdSP

Autorità di Sistema Portuale del Mare Adriatico Orientale.

LINEE GUIDA DI CONFINDUSTRIA

Le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. L.gs. 231/2001 approvate da Confindustria in data 7 marzo 2002 e successive modifiche ed integrazioni.

MODELLO

Il modello di organizzazione, gestione e controllo adottato da PTS sulla base delle disposizioni del D. L.gs. 231/2001.

CODICE ETICO

Il Codice Etico e di Comportamento adottato da PTS.

PROTOCOLLI 231

Procedure predisposte con specifico riferimento ad attività sensibili per la realizzazione dei reati previsti dal D. L.gs. 231/2001.

ORGANISMO DI VIGILANZA O ODV

Organismo preposto alla vigilanza sul funzionamento e sull'osservanza del Modello e al relativo aggiornamento.

P.A.

La Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio.

PARTNER O PARTNER COMMERCIALI

Controparti contrattuali di PTS quali, ad esempio, fornitori, agenti, System Integrator, sia persone fisiche sia persone giuridiche, con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (acquisto e cessione di beni e servizi, associazione temporanea d'impresa - ATI, Joint Venture, consorzi, ecc.), ove destinati a cooperare con il personale aziendale nell'ambito dei Processi Sensibili. Tra i fornitori di PTS.

PROCESSI SENSIBILI

Attività di PTS nel cui ambito ricorre il rischio di commissione dei Reati.

REATI

I reati ai quali si applica la disciplina prevista dal D. L.gs. 231/2001 (il cui elenco può anche essere eventualmente integrato in futuro).

PREMESSA

PTS è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali. A tal fine, sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, PTS ha avviato un Progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la rispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello possa costituire un valido strumento di sensibilizzazione di tutti coloro che operano in nome e per conto della Società, affinché tengano comportamenti corretti e lineari nell'espletamento delle proprie attività, tali da prevenire il rischio di commissione dei reati previsti dal Decreto stesso.

In particolare, attraverso l'adozione del Modello, PTS si propone di perseguire le seguenti principali finalità:

- Determinare, in tutti coloro che operano in nome e per conto della Società nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, nella commissione di illeciti passibili di sanzioni penali comminabili nei loro stessi confronti e di sanzioni amministrative irrogabili alla Società stessa;
- Ribadire che tali forme di comportamento illecito sono fortemente condannate dalla Società, in quanto le stesse (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche al "Codice Etico" al quale PTS intende attenersi nell'esercizio delle attività aziendali;
- Consentire alla Società, grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Nell'ottica della realizzazione di un programma d'interventi sistematici e razionali per l'adeguamento dei propri modelli organizzativi e di controllo, PTS ha predisposto una mappa delle attività aziendali e ha individuato nell'ambito delle stesse le cosiddette attività "a rischio" ovvero quelle che, per loro natura, rientrano tra le attività da sottoporre ad analisi e monitoraggio alla luce delle prescrizioni del Decreto.

A seguito dell'individuazione delle attività "a rischio", PTS ha ritenuto opportuno definire i principi di riferimento del Modello che intende attuare, tenendo presenti, oltre alle prescrizioni del Decreto, le linee guida elaborate in materia dalle associazioni di categoria.

PTS si impegna a svolgere un continuo monitoraggio della propria attività sia in relazione ai suddetti reati, sia in relazione all'espansione normativa cui potrà essere soggetto il D.Lgs 231/01. Qualora dovesse emergere la rilevanza di uno o più dei reati sopra menzionati, o di eventuali nuovi reati che il Legislatore riterrà di inserire nell'ambito del Decreto1, la Società valuterà l'opportunità di integrare il presente Modello con nuove misure di controllo e/o nuove Parti Speciali.

PARTE PRIMA

IL DECRETO LEGISLATIVO 231/2001

SOGGETTI, FATTISPECIE CRIMINOSE E SANZIONI

1.1. La Responsabilità amministrativa degli enti

Il Decreto Legislativo 8 giugno 2001, n. 231, avente ad oggetto la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nel nostro ordinamento la responsabilità degli Enti per gli illeciti amministrativi dipendenti da reato.

La disciplina è stata elaborata su impulso dell'Unione Europea e dell'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) che hanno emanato da tempo convenzioni in tema di lotta alla corruzione. Il legislatore italiano, con l'adozione del D. L.gs. 231/2001, emanato in attuazione dell'art. 11 della Legge delega 29 settembre 2000 n. 300, ha attuato la tutela internazionale per la lotta alla criminalità economica che vede l'Ente quale garante di interessi economici nei confronti dell'ordinamento statale e comunitario.

Si tratta di una particolare forma di responsabilità di natura amministrativa, che si sostanzia in una responsabilità penale a carico degli enti, accertata dinnanzi al giudice penale.

Il Decreto costituisce un intervento di grande portata normativa e culturale in cui, alla responsabilità penale della persona fisica che ha commesso il reato, si aggiunge quella dell'Ente a vantaggio o nell'interesse del quale lo stesso reato è stato perpetrato.

Le disposizioni contenute nel Decreto ai sensi dell'articolo 1, comma 2, si applicano ai seguenti "Soggetti":

• enti forniti di personalità giuridica;

• società e associazioni anche prive di personalità giuridica.

Ai sensi del successivo comma 3, restano invece esclusi dalla disciplina in oggetto:

• lo Stato;

• gli enti pubblici territoriali;

• gli altri enti pubblici non economici;

• gli enti che svolgono funzioni di rilievo costituzionale.

PTS in quanto Ente provvisto di personalità giuridica, rientra tra i soggetti ai quali si applica il regime della responsabilità amministrativa di cui al Decreto.

La responsabilità è attribuibile all'Ente ove i reati, indicati dal Decreto, siano stati commessi da soggetti legati a vario titolo all'Ente stesso.

Presupposto fondamentale della responsabilità è, quindi, la sussistenza di un legame funzionale o di subordinazione dell'autore del reato con l'Ente.

L'art. 5 del Decreto, infatti, indica quali autori del reato:

• i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale e coloro che esercitano, anche di fatto, la gestione ed il controllo dell'Ente (c.d. "soggetti apicali");

• i soggetti sottoposti alla direzione o alla vigilanza di soggetti apicali.

Nell'ipotesi di reati commessi da soggetto in posizione apicale, la responsabilità dell'Ente è esclusa qualora quest'ultimo dimostri che il reato è stato commesso eludendo fraudolentemente il modello di organizzazione e gestione esistente e che non vi sia stato, inoltre, omesso o insufficiente controllo da parte dell'organo responsabile 231.

Al contrario, nel caso di reato realizzato da soggetto in posizione subordinata, l'esclusione della responsabilità dell'Ente è subordinata all'adozione di protocolli comportamentali adeguati a garantire, per il tipo di organizzazione e di attività svolta, lo svolgimento dell'attività stessa nel rispetto della legge ed a verificare ed eliminare tempestivamente situazioni di rischio.

L'Ente, inoltre, sarà responsabile unicamente nel caso in cui la condotta illecita sia stata realizzata dai soggetti sopra indicati "nell'interesse o a vantaggio della società" (art. 5, comma 1, D. L.gs. 231/2001). Pertanto, non risponderà nell'ipotesi in cui i soggetti apicali od i dipendenti abbiano agito "nell'interesse esclusivo proprio o di terzi" (art. 5, comma 2, D. L.gs. 231/2001).

1.2. Definizione di rischio accettabile e fattispecie criminose

La responsabilità dell'Ente non è genericamente riferibile a qualsiasi reato, ma è circoscritta alle fattispecie criminose previste espressamente dal Decreto Legislativo 231/2001, nonché dall'art. 10 della Legge 16 marzo 2006, n.146, che ratifica e dà esecuzione alla Convenzione ed ai Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale.

Riguardo al sistema di controllo preventivo da costruire in relazione al rischio di commissione delle fattispecie di reati contemplate dal D. L.gs. 231/01, la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere raggirato se non in modo fraudolento

Questa soluzione è in linea con la logica della 'elusione fraudolenta' del modello organizzativo quale esimente espressa dal citato decreto legislativo ai fini dell'esclusione della responsabilità amministrativa dell'ente (Art. 6, Comma 1, Lettera c) "Le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione".

Diversamente, nei casi di reati di omicidio colposo e lesioni personali colpose commesse con violazione delle norme in materia di salute e sicurezza sul lavoro, la soglia concettuale di accettabilità, agli effetti esimente del D. L.gs. 231/01, è rappresentata dalla realizzazione di una condotta (non accompagnata dalla volontà dell'evento-morte/lesioni personali) contraria a quanto previsto nel modello organizzativo di prevenzione (e dei sottostanti adempimenti obbligatori prescritti dalle norme prevenzionistiche) nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal D. L.gs. 231/01 da parte dell'apposito organismo in quanto l'elusione fraudolenta dei modelli organizzativi appare incompatibile con l'elemento soggettivo dei reati di omicidio colposo e lesioni personali colpose, di cui agli artt. 589 e 590 del Codice Penale

In base al disposto del D. L.gs. 231/01 e successive integrazioni - la responsabilità amministrativa dell'ente si configura con riferimento alle seguenti fattispecie di reato:

REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE
Peculato (art.314 c.p.)
Malversazione a danno dello Stato o dell'Unione Europea (Art. 316 bis c.p.)
Indebita percezione di erogazioni a danno dello Stato (Art. 316 ter c.p.)
Truffa in danno dello Stato o di altro Ente Pubblico o dell'Unione Europea (Art. 640 – Comma 2, numero 1, c.p.)
Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640 bis)
Frode informatica in danno dello Stato o di altro Ente Pubblico (Art. 640 ter c.p.)
Concussione (Art. 317 c.p. modificato da L.69 del 27 maggio 2015.)
Corruzione per un atto d'ufficio – Corruzione per un atto contrario ai doveri d'ufficio –Circostanze aggravanti-Induzione indebita a dare o promettere utilità- Corruzione di persona incaricata di pubblico servizio (Artt. 318, 319 ,319 bis,319 quater e 320 c.p. modificati da L.69 del 27 maggio 2015)
Corruzione in atti giudiziari (Art. 319-ter c.p. modificato da L.69 del 27 maggio 2015)
Pene per il corruttore (Art.321 c.p.)
Istigazione alla corruzione (Art. 322 c.p.)
Peculato, concussione, corruzione ed istigazione alla corruzione di membri degli organi e di funzioni della comunità europee e di stati esteri (Art. 322 bis c.p.)

REATI SOCIETARI
False comunicazioni sociali (art. 2621, 2621 bis, 2621 ter c.c. modificati da L.69 del 27 maggio 2015)
Indebita restituzione dei conferimenti (art. 2626 c.c.)
Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)
Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Formazione fittizia del capitale (art.2632 c.p.)
Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
Corruzione tra privati (art.2635 c.c. modificato dal D. L.gs. n.201 del 29 ottobre 2016 e dal D.Lgs n.38 del 15 marzo 2017)
Istigazione alla corruzione tra privati (art.2635-bis c.c. introdotto dal D. L.gs n.38 del 15 marzo 2017)
Pene accessorie (art.2635-ter c.c. introdotto dal D. L.gs. n.38 del 15 marzo 2017)
Illecita influenza sull'assemblea (art. 2636 c.c.)
Aggiotaggio (art. 2637 c.c.)

REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI
Falsità in documenti informatici (art. 491-bis c.p. modificato da D. L.gs 7 del 15 gennaio 2016)
Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinqies c.p.)
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p. modificato da D. L.gs 7 del 15 gennaio 2016)
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. modificato da D. L.gs 7 del 15 gennaio 2016)
Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p. modificato da D. L.gs 7 del 15 gennaio 2016)
Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p. modificato da D. L.gs 7 del 15 gennaio 2016)
Frode informatica (art. 640-ter c.p.)
Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640-quinquies c.p.)

REATI AMBIENTALI
Inquinamento ambientale - (Art. 452 bis c.p. inserito da L. N 68 del 22 maggio 2015)

Disastro ambientale (Art 452 quater c.p. inserito da L. N 68 del 22 maggio 2015)
Delitti colposi contro l'ambiente- (Art. 452 quinquies c.p. inserito da L. N 68 del 22 maggio 2015)
Traffico e abbandono di materiale ad alta radioattività- (Art 452 sexies c.p. inserito da L. N 68 del 22 maggio 2015)
Circostanze aggravanti- (Art. 452 octies c.p. inserito da L. N 68 del 22 maggio 2015)
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.
Commercio internazionale delle specie di flora e di fauna selvatiche - Artt. 1, 2, 3bis e 6 L. n. 150/1992
Scarichi di acque reflue Sanzioni penali -Art. 137 D. L.gs. n. 152/2006
Attività di gestione di rifiuti non autorizzata- Art. 256 D. L.gs. n. 152/2006
Bonifica dei siti - Art.257 D. L.gs. n. 152/2006
Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari-Art.258 D. L.gs. n. 152/2006
Traffico illecito di rifiuti -Art. 259 D. L.gs. n. 152/2006
Attività organizzate per il traffico illecito di rifiuti-Art 260 D. L.gs. n. 152/2006
Sistema informatico di controllo della tracciabilità dei rifiuti -Art.260 bis D. L.gs. n. 152/2006
Sanzioni per superamento valori limite di emissione-Art. 279 D. L.gs. n. 152/2006
Inquinamento doloso provocato da navi -Art. 8 D. L.gs. n. 202/2007
Inquinamento colposo provocato da navi -Art. 9 D. L.gs. n. 202/2007
Cessazione e riduzione dell'impiego delle sostanze lesive - Art.3 Legge n. 549/1993

DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO
Turbata libertà dell'industria o del commercio (Art. 513 c.p.)
Illecita concorrenza con minaccia o violenza (Art. 513 bis c.p.)
Frodi contro le industrie nazionali (Art. 514 c.p.)
Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (Art. 517-ter c.p.)
Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (Art. 517 quater)

REATI FINANZIARI O ABUSI DI MERCATO
Reato di abuso di informazioni privilegiate – Art. 184 D. L.gs n.58/1998 (TUF)
Reato di manipolazione del mercato – Art. 185 D. L.gs n.58/1998 (TUF)
Illecito amministrativo di abuso di informazioni privilegiate – Art. 187-bis D. L.gs n.58/1998 (TUF)
Illecito amministrativo di manipolazione di mercato – Art.187-ter D. L.gs n.58/1998 (TUF)

REATI DI IMPIEGO DI LAVORATORI STRANIERI PRIVI DEL PERMESSO DI SOGGIORNO
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 22, comma 12 e 12-bis del D. L.gs. 286/98)

REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA
Ricettazione – Art. 648 c.p.
Riciclaggio – Art. 648-bis c.p. modificata dall'art. 3 della L. n.186 del 15 dicembre 2014
Impiego di denari, beni o utilità di provenienza illecita – Art. 648-ter c.p. modificata dall'art. 3 della L. n.186 del 15 dicembre 2014
Autoriciclaggio -Art 648-ter 1 c.p. inserito dalla Legge n.186 del 15 dicembre 2014

REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA
Reato di Induzione a non rendere dichiarazione o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 377-bis c.p.)

REATI TRANSNAZIONALI

Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D. L.gs. 25 luglio 1998, n. 286)
Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309)
Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43)
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)
Favoreggiamento personale (art. 378 c.p.)
Associazione per delinquere (Art. 416 c.p. modificato dalla legge 236 del 11 dicembre 2016)
Associazione di tipo mafioso (art. 416 bis c.p.)

1.3. La condizione esimente della responsabilità amministrativa dell'Ente

Istituita la responsabilità amministrativa degli Enti, l'art. 6 del Decreto stabilisce che l'Ente non ne risponde nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, "modelli di organizzazione di gestione e controllo idonei a prevenire reati della specie di quello verificatosi".

La medesima norma prevede, inoltre, l'istituzione di un organo di controllo interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei predetti modelli, nonché di curarne l'aggiornamento

Detti modelli di organizzazione, gestione e controllo (di seguito denominati i "Modelli"), ex art. 6, commi 2 e 3, del D. L.gs. 231/01, devono rispondere alle seguenti esigenze:

- Individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- Prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- Individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- Prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Ove il reato venga commesso da soggetti 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 soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'ente non risponde se prova che:

- L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;
- Il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- I soggetti hanno commesso il reato eludendo fraudolentemente il Modello;
- Non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo in ordine al Modello.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora

l'ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi

L'art.6 del Decreto dispone, infine, che i modelli di organizzazione e di gestione possano essere adottati sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia, il quale, di concerto con i Ministeri competenti, potrà formulare, entro 30 giorni, osservazioni sull'idoneità dei modelli a prevenire i reati.

1.4. Le Linee guida di Confindustria

Per espressa previsione legislativa (art. 6, comma 3, D. L.gs. 231/2001), i Modelli di organizzazione e di gestione possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia.

L'azienda aderisce a Confindustria, la quale in data 31 marzo 2008, ha emanato una versione aggiornata delle proprie "Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex D. L.gs. 231/01".

Il Ministero di Grazia e Giustizia in data 9 aprile 2008 ha approvato dette Linee Guida, ritenendo che l'aggiornamento effettuato sia da considerarsi "complessivamente adeguato ed idoneo al raggiungimento dello scopo fissato dall'art. 6 del Decreto".

Le Linee guida di Confindustria indicano un percorso che può essere in sintesi così riepilogato:

- Individuazione delle aree di rischio, al fine di evidenziare le funzioni aziendali nell'ambito delle quali sia possibile la realizzazione degli eventi pregiudizievoli previsti dal Decreto;
- Predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di appositi protocolli.

Le componenti più rilevanti del sistema di controllo ideato da Confindustria sono:

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

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

- Verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- Applicazione del principio di segregazione dei compiti;
- Documentazione dei controlli;
- Previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure.

Individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili in:

- Autonomia e indipendenza;

- Professionalità;
- Continuità di azione;
- Previsione di modalità di gestione delle risorse finanziarie;
- Obblighi di informazione dell'organismo di controllo.

Il mancato rispetto di punti specifici delle predette Linee Guida non inficia la validità del Modello. Infatti, il Modello adottato dall'Ente deve essere necessariamente redatto con specifico riferimento alla realtà concreta della Società, e pertanto lo stesso può anche discostarsi dalle Linee Guida di Confindustria, le quali, per loro natura, hanno carattere generale.

Tali linee guida in quanto naturale punto di riferimento per i modelli delle singole imprese anche se non materialmente allegate al presente Modello ne fanno parte integrante nella versione più aggiornata disponibile.

PARTE SECONDA

IL MODELLO ORGANIZZATIVO DI PORTO DI TRIESTE SERVIZI S.r.l.

2.1. Elementi fondamentali del Modello

Con riferimento alle "esigenze" individuate dal legislatore nel Decreto Legislativo 231/2001, i punti fondamentali individuati da PTS nella definizione del Modello possono essere così brevemente riassunti:

- Mappa delle attività aziendali "sensibili" ovvero di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto e pertanto da sottoporre ad analisi e monitoraggio;
- Analisi dei protocolli in essere e definizione delle eventuali implementazioni finalizzate, con riferimento alle attività aziendali "sensibili", a garantire i principi di controllo;
- Modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- Identificazione dell'Organismo di Vigilanza, ruolo attribuito a professionisti indipendenti esterni con attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- Definizione dei flussi informativi nei confronti dell'Organismo di Vigilanza;
- Attività di informazione, sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- Definizione delle responsabilità nell'approvazione, nel recepimento, nell'integrazione e nell'implementazione del Modello, oltre che nella verifica del funzionamento dei medesimi e dei comportamenti aziendali con relativo aggiornamento periodico (controllo ex post);

Si rileva, ad ogni modo, che il modello organizzativo previsto dal D. L.gs. 231/01 non costituisce, per la Società, nulla di nuovo poiché l'attività svolta è sostanzialmente caratterizzata da un proprio sistema di controllo particolarmente rigoroso basato sull'implementazione e l'attuazione del Sistema di Gestione delle problematiche relative alla Qualità in accordo alle norme:

- **UNI EN ISO 9001:2015**

Ulteriormente PTS assicura che, il trattamento dei dati personali avviene in conformità al D. L.gs. 196/03 e al GDPR Regolamento UE 2016/679.

2.2. Modello, Codice Etico e sistema disciplinare

PTS ha ritenuto opportuno formalizzare i principi etici a cui la stessa quotidianamente si ispira nella gestione delle attività aziendali all'interno di un Codice Etico, in considerazione anche dei comportamenti che possono determinare la commissione dei reati previsti dal Decreto.

Gli obiettivi che la Società ha inteso perseguire mediante la definizione del Codice Etico possono essere così riepilogati:

- Improntare su principi di correttezza e trasparenza i rapporti con le terze parti ed in particolar modo con la Pubblica Amministrazione;

- Richiamare l'attenzione del personale dipendente, dei collaboratori, dei fornitori, e, in via generale, di tutti gli operatori, sul puntuale rispetto delle leggi vigenti, delle norme previste dal Codice etico, nonché delle procedure a presidio dei processi aziendali;
- Definire un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

I principi di riferimento del Modello si integrano con quelli del Codice Etico adottato dalla Società, per quanto il Modello, per le finalità che lo stesso intende perseguire in specifica attuazione delle disposizioni del Decreto, abbia una diversa portata rispetto al Codice Etico.

Sotto tale profilo, infatti, è opportuno precisare che:

- Il Codice Etico riveste una portata generale in quanto contiene una serie di principi di "deontologia aziendale" che la Società riconosce come propri e sui quali intende richiamare l'osservanza di tutti i suoi dipendenti e di tutti coloro che cooperano al perseguimento dei fini aziendali;
- Il Codice Etico rimanda al sistema disciplinare aziendale atto a sanzionare il mancato rispetto delle misure indicate nel Modello, previsto all'art. 6, comma 2 lett. e) del Decreto;
- Il Modello risponde, invece, a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati per fatti che, commessi nell'interesse o a vantaggio della Società, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo.

2.3. Politica integrata con il Sistema di Gestione della Qualità (SGR)

PTS ha elaborato Il presente Modello in modo che lo stesso si integri con il Sistema Qualità la cui certificazione è stata ottenuta, per la prima volta in data 24.01.2011 e, successivamente, aggiornata secondo lo standard ISO 9001 – 2015.

Nel contesto del sistema sopra indicato è stato inserito il Codice Etico di comportamento nel quale sono rappresentati i principi generali di trasparenza, correttezza e lealtà cui si ispirano lo svolgimento e la conduzione delle attività

La politica integrata è condivisa con tutto il personale.

PTS si impegna a:

- Promuovere la formazione continua dei dipendenti
- Diffondere la politica a tutti i livelli ed alle parti interessate
- Essere al fianco del cliente per assisterlo e supportarlo nella propria attività
- Diffondere ed accrescere presso i clienti la cultura dei sistemi di gestione integrata

Il coinvolgimento del personale, la sua motivazione e la formazione continua sono presupposti indispensabili per il successo dell'attività aziendale.

PTS crede che un Sistema di Gestione per la Qualità porti valore aggiunto creando l'interfaccia con strumenti di controllo di gestione che permettano di attribuire valori economici a tutti i dati aziendali. I dati raccolti con sistematicità attraverso gli strumenti del SGQ permetteranno di definire scelte operative e strategiche al fine di:

- Garantire un miglioramento continuo del SGQ
- Garantire la soddisfazione del cliente interno ed esterno
- Valorizzare le segnalazioni del cliente per un'attenta analisi e precisa soluzione dei reclami
- Conseguire una crescita etica senza rinunciare ad un adeguato utile operativo netto

PARTE TERZA

PORTO DI TRIESTE SERVIZI S.r.l.

3.1. La storia e lo sviluppo della Società

La società Porto di Trieste Servizi S.p.A. è stata costituita, con Deliberazione del Comitato Portuale n. 1 del 20 gennaio 2009 e successiva Deliberazione del Presidente dell'Autorità Portuale di Trieste n. 23 del 23 gennaio 2009, per la gestione dei servizi di interesse generale di cui all'articolo 1, lettera a), b), c), d), f), g) del D.M. 14 novembre 1994, in attuazione della Legge n. 84/1994.

A seguito del parere favorevole espresso dalla competente Direzione Generale del Ministero delle Infrastrutture e dei Trasporti (prot. gen. 6123/A del 20 luglio 2015), con Deliberazione del Comitato Portuale n. 15 del 25 novembre 2015, l'Autorità Portuale è stata autorizzata all'adozione di "*tutti gli atti necessari alla trasformazione della predetta partecipata in società "in house""*, oltre che all'affidamento "*da parte dell'Autorità Portuale – a mente dell'articolo 6, comma 1° lett. c) e comma 5° della legge n. 84/1994 – dei servizi che, a seguito della trasformazione di cui al precedente punto 1), non potranno essere svolti dalla Porto di Trieste Servizi S.p.A.*" .

Con la modifica statutaria prevista nella citata Deliberazione, l'Autorità Portuale ha affidato alla Porto di Trieste Servizi S.p.A. la fornitura di servizi, in via diretta ed esclusiva, a favore dell'Autorità stessa realizzando, così, il duplice obbiettivo di mantenere, da un lato, nell'ambito del controllo diretto dell'Autorità l'insieme dei servizi strategici e di interesse generale idonei a determinare un vantaggio competitivo per il Porto di Trieste e, dall'altro, di avvantaggiarsi della maggiore elasticità, propria delle società, nella gestione e nell'implementazione dei servizi in funzione dell'evoluzione delle necessità e delle richieste degli operatori, mantenendo, comunque, il "*know how*" relativo alle infrastrutture ed ai servizi all'interno dell'Autorità Portuale.

La trasformazione di Porto di Trieste Servizi S.P.A. in società "*in house"* ha, altresì, assicurato, insieme alla tempestività ed alla qualità nell'erogazione dei servizi, proprio in considerazione della maggiore flessibilità nell'utilizzo del personale e alla copertura delle esigenze, l'economicità dei servizi svolti quale effetto sia del rapporto diretto con l'Autorità Portuale quanto dell'ottimizzazione delle risorse interne.

Nell'ambito della illustrata razionalizzazione e al fine di raggiungere maggiori livelli di efficienza ed efficacia delle attività svolte a favore del Socio Unico, oggi Autorità di Sistema Portuale del Mare Adriatico Orientale (Autorità), oltre che per garantire la massima economicità dei servizi, l'Assemblea straordinaria della Porto di Trieste Servizi S.p.A. ha deliberato, in data 23 maggio 2018, la trasformazione dalla forma azionaria a quella di società a responsabilità limitata, in quanto più funzionale alle esigenze aziendali, con la nuova denominazione "Porto di Trieste Servizi S.r.l." (PTS), mantenendo il capitale sociale versato ed approvando, di conseguenza, il testo del nuovo Statuto societario.

In detta occasione, essendosi concluso il mandato dell'Amministratore Unico e del Collegio Sindacale, con l'approvazione del bilancio chiuso al 31 dicembre 2017, l'Assemblea ordinaria della Porto di Trieste Servizi ha deliberato di affidare l'amministrazione della società ad un Consiglio di Amministrazione composto da tre membri che, in prima battuta, sono rimasti in carica fino all'approvazione, da parte dell'Assemblea, del bilancio di esercizio al 31 dicembre 2018 e sono stati, in quella sede, confermati sino ad approvazione del bilancio di esercizio al 31 dicembre 2021.

L'adozione di un organo di amministrazione di natura collegiale risulta giustificato in considerazione dell'incremento della complessità delle attività affidate dal D.lgs. 4 agosto 2016, n. 169 all'Autorità di Sistema Portuale, rispetto a quelle precedentemente svolte dall'Autorità Portuale, con conseguente incremento delle attività affidate alla società "*in house*", quale braccio operativo dell'Autorità stessa.

L'affidamento dell'amministrazione della Porto di Trieste Servizi S.r.l. ad un Consiglio di Amministrazione risulta, così, soddisfare compiutamente l'esigenza di rappresentare all'interno dell'organo di amministrazione la complessità delle predette attività.

Proprio l'incremento delle attività affidate a PTS dall'Autorità ha reso, altresì, necessaria una riorganizzazione interna delle competenze e delle funzioni con l'obbiettivo di realizzare una struttura in grado di rispendere prontamente ed efficacemente alle esigenze della controllante.

A fini di contenimento di costi è invece indirizzata la disposta riduzione del collegio sindacale in organo monocratico.

La detta riorganizzazione, che attualmente risulta ancora in fase di definizione, necessita di un periodo di implementazione alla quale seguirà una fase di verifica dell'efficacia degli interventi e, nel caso, di successive correzioni a valle.

Se, quindi, l'anno 2018 è stato l'anno della trasformazione societaria, il 2019 si presenta quale anno destinato alla riorganizzazione aziendale ed alla implementazione del nuovo assetto organizzativo.

Alla luce di quanto sopra ne consegue che, il presente Modello Organizzativo che trova la propria giustificazione sulla mappatura dei rischi derivati dall'analisi di una struttura organizzativa oggetto di possibili modifiche, necessiterà, una volta approvata, di una particolare attività di monitoraggio al fine di verificarne l'effettiva e costante corrispondenza ai mutamenti organizzativi aziendali.

Per la detta ragione il C.d.A., approvando il presente Modello organizzativo, ritiene opportuno prevedere, sin d'ora, una fase di verifica, da effettuarsi al termine del primo semestre dall'approvazione del Modello stesso, degli effetti della riorganizzazione sulla esposizione della società ai rischi reato ex D.Lgs 231/01 con l'obbiettivo di effettuare una valutazione ed una ponderazione del rischio che non si risolva nella mera applicazione meccanica di modelli predefiniti ma che predisponga, a valle della fase di riorganizzazione societaria ed aziendale, una nuova mappatura degli stessi al fine di permettere la verifica dell'efficacia e della coerenza degli strumenti di prevenzione adottati e, conseguentemente, l'adeguatezza del Modello stesso.

Si ritiene opportuno evidenziare che, Il capitale sociale è interamente detenuto dall' Autorità la quale esercita su PTS un controllo analogo a quello che la medesima esercita sui propri servizi.

Il capitale della società è incedibile e la società in house non svolge attività ulteriori rispetto a quelle affidatele dalla stessa Autorità, se non nella misura contenuta entro il 20% del proprio fatturato, secondo quanto stabilito dalla disciplina normativa di matrice comunitaria vigente in materia.

Quanto ai rapporti intercorrenti tra l'Autorità e PTS deve osservarsi che gli stessi trovano fondamento nelle tre Convenzioni denominate "Convenzione Quadro" (avente natura generale) "Convenzione Manutenzioni" e "Convezione Servizi". Le Convenzioni afferenti le manutenzioni e i servizi stabiliscono i livelli di servizio essenziali richiesti nello svolgimento delle attività.

Da ultimo si segnala che, a seguito dell'indagine compiuta dall'Autorità secondo il dettato normativo di cui al D.lgs. n. 175/2016, la stessa ha ritenuto opportuno il mantenimento della partecipazione in relazione alla gestione di un servizio di interesse generale, ex articolo 4, comma 2, lett. a) D.lgs. n. 175/2016, da parte di PTS e nella mancata rilevazione della sussistenza delle condizioni di cui all'articolo 20, comma 2, D.lgs. n. 175/2016.

3.2. Governance

Il Decreto Legislativo 231/2001 non ha modificato il sistema normativo che disciplina l'amministrazione ed il governo delle società, sicché l'autonomia decisionale dei soggetti posti al vertice aziendale è sostanziale ed indefettibile espressione della libertà di gestione dell'impresa in forma societaria.

Per quanto riguarda in particolare gli assetti della Governance di PTS, il Consiglio di Amministrazione, secondo quanto stabilito nello statuto sociale, agisce nel rispetto degli indirizzi e delle istruzioni deliberate dall'Assemblea.

In particolare, l'organo amministrativo è responsabile dell'attività societaria nei confronti del Socio unico e garantisce la piena rispondenza dei risultati delle attività e della gestione societaria alle finalità dello Statuto, agli obiettivi, alle direttive ed alle istruzioni definite dal Socio Unico.

L'organo amministrativo è investito di ogni potere dal Socio Unico per l'amministrazione della società e provvede a tutto quanto non sia riservato dalla legge o dallo Statuto alle determinazioni del Socio Unico.

Sono, in particolare, di competenza dell'organo amministrativo I poteri e le attribuzioni relativi a:

a) proposte all'approvazione del Socio Unico di regolamenti interni e delle norme generali per l'esercizio delle attività sociali;

b) predisposizione del bilancio d'esercizio e dei relativi allegati, nonché della relazione sulla gestione nei termini previsti dalla legge;

c) predisposizione di programmi di attività della Società, in conformità agli indirizzi ed alle istruzioni dettate dal Socio Unico;

d) poteri di direzione del personale per l'espletamento delle attività della Società anche in riferimento all'organizzazione del lavoro e alle modalità di espletamento dei servizi.

Gli amministratori devono invece richiedere la preventiva autorizzazione da parte del Socio Unico per il compimento delle seguenti operazioni:

a) sviluppo di nuove attività e/o di nuovi servizi e/o acquisizione e/o dismissione di attività o servizi già esercitati;

b) acquisti e/o alienazioni di immobili, di impianti, di partecipazioni, di aziende e/o rami d'azienda;

c) rilascio di garanzie superiori a euro 50.000,00 (cinquantamila/00);

d) nomina di un Amministratore Delegato;

e) conferimento di attività sociali in altre società o consorzi;

f) regolamenti su assunzioni, acquisti e forniture, gare e conferimento di incarichi e consulenze di qualsiasi tipo.

Sono inderogabilmente riservate alla competenza dell'Assemblea dei soci:

a) l'approvazione del bilancio;

b) la nomina e la revoca dell'Organo di Amministrazione;

c) la nomina dei Sindaci e del Presidente del Collegio Sindacale ovvero del Sindaco Unico;

d) la nomina del revisore legale dei conti;

e) la determinazione del compenso degli Amministratori, ove consentito, e dei Sindaci;

f) deliberazione sulla responsabilità degli Amministratori e dei Sindaci;

g) operazioni per le quali è necessaria la preventiva autorizzazione del Socio Unico.

In ogni caso, sono riservate alla competenza dell'Assemblea le decisioni sugli argomenti di cui all'art. 2479 c.c., comma 2 e comunque:

a) decisioni relative alla strategia di programmazione;

b) eventuali modifiche degli organi della società;

c) approvazione dei regolamenti interni e delle norme generali per l'esercizio delle attività sociali;

d) definizione di indirizzi ed istruzioni vincolanti per l'attività dell'organo amministrativo;

e) approvazione degli atti di programmazione, dei piani operativi annuali, sulla base dei quali si svilupperà l'azione societaria, dei piani di investimento e di quelli di assunzione del personale;

f) prestazioni di garanzie, fidejussioni e concessioni di prestiti nonché la concessione di diritti reali di garanzia su beni immobili;

g) assunzione di prestiti e/o finanziamenti superiori a euro 50.000,00 (cinquantamila/00).

Sono altresì di competenza dell'Assemblea:

a) l'aumento del capitale sociale;

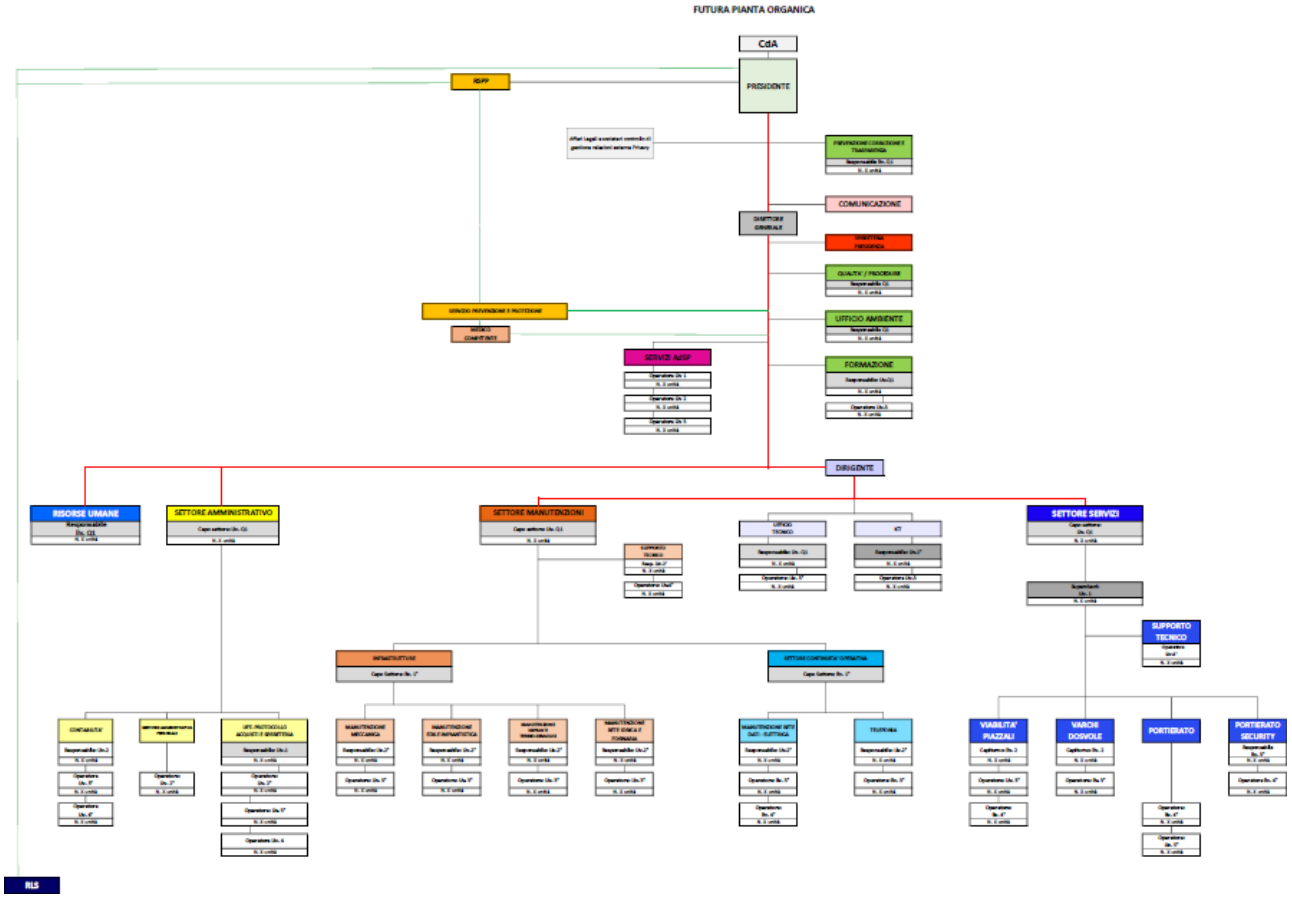
b) le modifiche dello statuto, salvo quanto previsto dallo statuto;

c) la nomina, la sostituzione e la determinazione dei poteri dei Liquidatori;

d) le altre materie ad essa attribuite dalla legge e dallo statuto.

L'eventuale attribuzione all'organo amministrativo della competenza a deliberare su materie che per legge spettano all'Assemblea non fa venire meno la competenza principale dell'Assemblea, che mantiene il potere concorrente di deliberare in materia.

3.3. Organigramma



Aggiornato al 14 giugno 2019 e soggetto all'approvazione di AdSP.

PARTE QUARTA

LA COSTRUZIONE DEL MODELLO

4.1. Struttura del Modello

Il Modello intende uniformare il sistema aziendale di prevenzione e gestione dei rischi alle disposizioni ed allo spirito del D. L.gs. 231/2001.

La redazione del Modello è stata condotta sulla base degli aggiornamenti apportati al Decreto, dei principali casi giudiziari accertati, delle opinioni dottrinali, delle best practice adottate dalle principali società nonché sulle principali normative anche volontarie che indicano principi guida e standard di controllo per un sistema di organizzazione interno. Il tutto tenendo in debito conto del ridotto numero degli addetti e del cospicuo volume d'affari.

Le attività considerate rilevanti ai fini della predisposizione del Modello sono quelle che, a seguito di specifica analisi dei rischi, hanno manifestato fattori di rischio relativi alla commissione di violazioni delle norme penali indicate dal D. L.gs. 231/01 o, in generale, dal Codice Etico della Società stessa.

In tal senso è stata creata la seguente tabella per poter valutare questi aspetti e definirne delle priorità di intervento.

	Probabilità "**P**"	Danno "**D**"	**Valore**
Inevitabile	**≥ 30%**	**Altissimo**	**5**
Alta	**5% ≤ P < 30%**	**Alto**	**4**
Moderata	**1% ≤ P < 5%**	**Moderato**	**3**
Bassa	**0,01% ≤ P < 1%**	**Basso**	**2**
Remota	**< 0,01%**	**Irrilevante**	**1**

P x D	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Se P x D	**0 – 5**	**Nessuna azione**
Se P x D	**6 – 10**	**Azione necessaria entro 1 anno**
Se P x D	**11 – 16**	**Azione necessaria entro 1 mese**
Se P x D	**17-25**	**Azione necessaria entro 2 giorni**

L'analisi dei rischi è stata strutturata in modo da valutare per ciascuna fase dei processi, quali possono essere quelli potenzialmente a rischio relativamente ai singoli articoli del D. L.gs. 231/01.

Le principali aree di attività potenzialmente a rischio sono elencate nelle parti speciali del Modello.

Si precisa che i reati di cui all'art. 25-septies del Decreto (omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme in materia di salute e sicurezza sul lavoro) per loro natura possono essere riferibili a tutte le aree aziendali.

PTS si è dotata di una politica aziendale in materia di sicurezza ed igiene del lavoro e delle strutture di prevenzione e protezione previste dalla normativa di riferimento (Legge 123/2007 e D. L.gs. 81/08 e successive modifiche).

4.2. Principi di controllo nelle potenziali aree di attività a rischio

Nell'ambito dello sviluppo delle attività di definizione dei protocolli necessari a prevenire le fattispecie di rischio-reato, sono stati individuati, sulla base della conoscenza della struttura interna e della documentazione aziendale, i principali processi, sotto processi o attività nell'ambito dei quali, in linea di principio, potrebbero realizzarsi i reati o potrebbero configurarsi le occasioni o i mezzi per la realizzazione degli stessi.

Con riferimento a tali processi, sotto processi o attività è stato rilevato il sistema di gestione e di controllo in essere focalizzando l'analisi sulla presenza/assenza all'interno dello stesso dei seguenti elementi di controllo:

- **Regole comportamentali**: esistenza di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi, dei regolamenti e dell'integrità del patrimonio aziendale
- **Procedure**: esistenza di procedure interne a presidio dei processi nel cui ambito potrebbero realizzarsi le fattispecie di reati previste dal D. L.gs. 231/01 o nel cui ambito potrebbero configurarsi le condizioni, le occasioni o i mezzi di commissione degli stessi reati.

Le caratteristiche minime che sono state esaminate sono:

- Definizione e regolamentazione delle modalità di svolgimento delle attività;
- Tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali che attestino le caratteristiche e le motivazioni dell'operazione ed individuino i soggetti a vario titolo coinvolti nell'operazione (autorizzazione, effettuazione, registrazione, verifica dell'operazione);
- Esistenza di criteri oggettivi per l'effettuazione delle scelte aziendali;
- Adeguata formalizzazione e diffusione delle procedure aziendali.

La recente trasformazione aziendale, l'affidamento di sempre più rilevanti e consistenti attività operative da parte di AdSP, conseguenza delle aumentate aree di competenza di quest'ultima, hanno comportato la necessità per PTS di implementare una struttura sempre più complessa in grado di soddisfare le molteplici e diverse esigenze rappresentate dal Socio Unico.

Sintomo evidente di detto aumento delle attività è l'incremento di personale che è passato da 15 unità (31 dicembre 2015) a 72 (31 dicembre 2018).

Tanto ha comportato la necessità di elaborare una nuova ripartizione dei compiti e delle attività ed una conseguente concreta segregazione dei compiti e delle responsabilità.

La struttura aziendale precedente, caratterizzata dal rapporto diretto tra il centro decisionale e gli addetti operativi è risultata, infatti, inadeguata a soddisfare le nuove esigenze aziendali.

Ad oggi, però, la presenza di un unico centro decisionale e la limitata presenza di una struttura dirigenziale intermedia – individuabile nel Direttore Generale – pur coniugando la capacità e l'esperienza maturata nel settore appare insoddisfacente.

Per le dette ragioni PTS, oltre a aver identificato le soluzioni possibili, implementando diversi livelli autorizzativi (rappresentativi dei poteri e delle responsabilità riferibili alle mansioni attribuite e alle posizioni ricoperte nell'ambito della struttura organizzativa), ha ritenuto opportuno concentrarsi anche sulle attività di controllo, anche preventivo, e di monitoraggio che sono svolte dall'Organo di Amministrazione con il supporto di soggetti indipendenti esterni alla organizzazione aziendale (Collegio Sindacale, Organismo di Vigilanza e Controllo Analogo di AdSP).

In considerazione dei poteri attribuiti agli organi societari, si è ritenuto che la figura apicale di riferimento al fine del Modello 231 sia identificabile nel Consiglio di Amministrazione il quale, in via ordinaria, decide operazioni che seguono i normali criteri previsti dal Modello.

Pur tuttavia talvolta si rende necessario - nell'interesse della Società - avviare operazioni che seguono un iter procedimentale diverso da quello dettagliato nel Modello, a causa di situazioni di eccezionalità dovute ad esigenze di straordinaria urgenza o di particolare riservatezza od anche di singola peculiarità dell'operazione.

In tal ultimo caso, il sistema di controllo si basa sui due elementi qualificanti della tracciabilità degli atti e del flusso informativo verso l'Organismo di Vigilanza.

In particolare, gli elementi specifici di controllo sono:

- Tracciabilità dell'operazione in termini di documentazione e supporti informativi atti a consentire la "ricostruibilità" a posteriori delle motivazioni e delle situazioni contingenti in cui si è sviluppata l'operazione stessa;
- Speciale riguardo deve assumere l'esplicazione, ancorché in forma sintetica (ma non generica), delle ragioni e dei motivi che hanno determinato la scelta operativa. Non necessariamente devono essere esplicitate le ragioni della decisione, ma le caratteristiche (ad esempio: riservatezza ed urgenza) che hanno reso impossibile l'attuazione della decisione secondo lo schema operativo prefissato;
- Specifica informativa, da parte dello stesso soggetto di vertice che ha attivato l'operazione "in deroga", verso l'Organismo di Vigilanza affinché possa attuare i dovuti riscontri con sistematicità e tempestività; l'assenza di operazioni in deroga nel periodo di riferimento dovrà comunque essere oggetto di specifica informativa all'Organismo di Vigilanza da parte del soggetto di vertice.

Il riesame della procedura di controllo è responsabilità del Consiglio di Amministrazione che annualmente verifica lo stato di applicazione del Modello e propone le possibili azioni di miglioramento dello stesso.

Nell'ambito delle iniziative attuate dal C.d.A., allo scopo di diversificare i livelli autorizzativi e di responsabilità e sviluppare forme di controllo sulle attività soggette a rischio 231, deve segnalarsi l'adozione del Regolamento assunzioni e del Regolamento acquisti. Atti, questi, preventivamente autorizzati dall'Ufficio del Controllo analogo di AdSP.

A ciò deve aggiungersi che PTS sta predisponendo un sistema di controllo di gestione che verrà, probabilmente, implementato per la fine dell'anno 2019 e che garantirà un ancor maggior controllo – anche di tipo preventivo - sulle attività svolte permettendo, altresì, la predisposizione di programmi di spesa e di miglior utilizzo delle risorse.

4.3. Misurazioni, analisi e miglioramenti

PTS al fine di pianificare ed attuare i processi di analisi e di miglioramento necessari a dimostrare l'adeguatezza del Modello, assicurarne la conformità alla legislazione vigente e migliorarlo continuamente ha ritenuto opportuno prevedere le seguenti azioni:

- Previsione di un programma di audit finalizzato alla promozione di azioni correttive e preventive;
- Analisi e gestione delle non conformità;
- Monitoraggio delle informazioni relative alla percezione e al grado di coinvolgimento delle parti interessate sull'importanza e corretta implementazione del Modello.

L'analisi dei dati del monitoraggio e misurazione dei processi permette di dimostrare l'adeguatezza e l'efficacia del Modello e la valutazione delle aree dove possa essere realizzato il miglioramento continuo e fornisce informazioni in merito a:

- Percezione e grado di coinvolgimento delle parti interessate
- Conformità alle prescrizioni legali
- Caratteristiche e tendenze dei processi, comprese opportunità per azioni preventive

L'organizzazione al fine di migliorare in continuo l'efficacia del SGRA utilizza i seguenti strumenti:

- Politica per la responsabilità amministrativa
- Codice Etico
- Risultati degli audit
- Analisi dei dati
- Azioni correttive e preventive.

PARTE QUINTA

L'ORGANISMO DI VIGILANZA

5.1. I requisiti

L'art. 6, comma 1, lett. b), del D. L.gs. n. 231/01, individua l'istituzione di un Organismo di Vigilanza, come requisito affinché l'ente possa essere esonerato dalla responsabilità "amministrativa" dipendente dalla commissione dei reati specificati nel D. L.gs. stesso.

I requisiti che l'organo di controllo deve soddisfare per un efficace svolgimento delle predette funzioni sono:

- Autonomia ed indipendenza: l'Organismo di Vigilanza deve essere sprovvisto di compiti operativi e deve avere solo rapporti di staff - come meglio si dirà in seguito - con il vertice operativo aziendale e con Il Consiglio di Amministrazione;
- Professionalità nell'espletamento dei suoi compiti istituzionali; a tal fine i componenti del suddetto organo devono avere conoscenze specifiche in relazione a qualsiasi tecnica utile per prevenire la commissione di reati, per scoprire quelli già commessi e individuarne le cause, nonché per verificare il rispetto dei modelli da parte degli appartenenti all'organizzazione aziendale;
- Continuità di azione, al fine di garantire la costante attività di monitoraggio e di aggiornamento del Modello e la sua variazione al mutare delle condizioni aziendali di riferimento.

5.2. Individuazione

In considerazione delle caratteristiche sopra evidenziate, della specificità dei compiti assegnati all'Organismo di Vigilanza, nonché dell'attuale struttura organizzativa adottata dalla Società, si ritiene opportuno identificare e regolamentare tale organismo come segue:

- L'Organismo di Vigilanza ha una struttura collegiale composta da un Presidente e due membri;
- Il Consiglio di Amministrazione, al fine di garantire la presenza dei requisiti sopra menzionati, valuta periodicamente l'adeguatezza dell'Organismo di Vigilanza in termini di struttura organizzativa e di poteri conferiti, apportando le modifiche e/o le integrazioni ritenute necessarie
- L'Organismo di Vigilanza è configurato come unità di staff in posizione verticistica, riportando direttamente al Consiglio di Amministrazione.

Il funzionamento dell'Organismo di Vigilanza è disciplinato da un apposito Regolamento, predisposto dall'Organismo medesimo ed approvato dal Consiglio di Amministrazione. Tale regolamento prevede, tra l'altro, le funzioni, i poteri e i doveri dell'Organismo, nonché i flussi informativi verso il Consiglio di Amministrazione. Sotto questo profilo è opportuno prevedere che ogni attività dell'Organismo di Vigilanza sia documentata per iscritto ed ogni riunione o ispezione cui esso partecipi sia opportunamente verbalizzata.

5.3. Nomina

Il Consiglio di Amministrazione della Società provvede alla nomina dell'Organismo di Vigilanza secondo le indicazioni fornite dal Socio Unico.

La durata in carica dei componenti dell'Organismo di Vigilanza è stabilita dal Consiglio di Amministrazione della Società.

L'Organismo di Vigilanza è dotato ai sensi dell'art. 6, comma 1, lett. b), del D. L.gs. 231/01 di "autonomi poteri di iniziativa e controllo".

La nomina quale componente dell'Organismo di Vigilanza è condizionata all'assenza dei motivi di ineleggibilità, quali:

- L'esistenza di relazioni di parentela, coniugio;
- Affinità entro il IV grado con componenti del Consiglio di Amministrazione titolari di deleghe esecutive, sindaci della Società e revisori incaricati dalla Società di revisione;
- La titolarità di conflitti di interesse con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'Organismo di Vigilanza;
- La titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza sulla Società;
- L'aver svolto un rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell'Organismo di Vigilanza ovvero all'instaurazione del rapporto di consulenza/collaborazione con lo stesso Organismo;
- L'aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento), in Italia o all'estero, per delitti dolosi richiamati dal D. L.gs. 231/2001 od altri delitti comunque incidenti sulla moralità professionale;
- L'aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero con provvedimento che comunque ne accerti la responsabilità, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi in capo ad un soggetto già nominato, opererà una decadenza automatica.

Il Consiglio di Amministrazione può disporre con adeguata motivazione e sentito il Collegio Sindacale la revoca del mandato esclusivamente nel caso di grave inadempimento dei compiti affidati ai componenti dell'Organismo di Vigilanza.

Il Consiglio di Amministrazione stabilisce il compenso per i componenti dell'Organismo di Vigilanza.

In caso di rinuncia, sopravvenuta incapacità o decadenza dell'Organismo, questi ne darà comunicazione tempestiva al Consiglio di Amministrazione il quale provvederà senza indugio alla sua sostituzione. É fatto obbligo all'Organismo di Vigilanza comunicare tempestivamente al Consiglio di Amministrazione il verificarsi di una delle ipotesi dalle quali derivi la necessità di sostituirlo.

5.4. Funzioni

In base a quanto emerge dal testo del D. L.gs. 231/01, le funzioni svolte dall'Organismo di Vigilanza possono essere così riepilogate:

- Vigilanza sull'effettività del Modello: che consiste nel verificare la coerenza tra comportamenti concreti e Modello istituito;
- Valutazione dell'adeguatezza del Modello: ossia della idoneità dello stesso, in relazione alla tipologia di attività e alle caratteristiche dell'impresa, a ridurre ad un livello accettabile i rischi di realizzazione di reati. Ciò impone un'attività di aggiornamento del Modello sia alle mutate realtà organizzative aziendali, sia ad eventuali mutamenti della legge in esame. L'aggiornamento può essere proposto dall'Organismo di Vigilanza, ma deve essere adottato - come già ricordato - dall'organo amministrativo,

In particolare, i compiti dell'Organismo di Vigilanza sono così definiti:

- Vigilare sull'effettività del Modello attuando le procedure di controllo previste;
- Verificare l'efficacia nel prevenire i comportamenti illeciti;
- Verificare il mantenimento, nel tempo, dei requisiti richiesti promuovendo, qualora necessario, il necessario aggiornamento;
- Promuovere e contribuire, in collegamento con le altre unità interessate, all'aggiornamento e adeguamento continuo del Modello e del sistema di vigilanza sull'attuazione dello stesso;
- Assicurarsi i flussi informativi di competenza;
- Assicurare l'attuazione degli interventi di controllo programmati e non programmati;
- Segnalare alle funzioni competenti la notizia di violazione del Modello e monitorare l'applicazione delle sanzioni disciplinari;

Nell'espletamento delle sue funzioni, l'Organismo di Vigilanza ha la facoltà di:

- Emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'Organismo di Vigilanza;
- Accedere a qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo di Vigilanza ai sensi del D. L.gs. n. 231/01;
- Ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
- Disporre che i Responsabili delle funzioni aziendali forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello.

L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione e potrà, a sua volta, chiedere di essere ascoltato in qualsiasi momento, al fine di riferire sul funzionamento del Modello o su situazioni specifiche.

L'Organismo di Vigilanza, anche avvalendosi della collaborazione di consulenti esterni, si attiva con specifiche operazioni di audit sulle realtà della Società, laddove coinvolte, con le seguenti modalità:

- Con interventi "a piano", nei quali le attività di controllo relative all'efficacia del Modello sono parte integrante di un piano di lavoro più ampio; in questo tale attività viene specificatamente considerata e adeguatamente valorizzata, di concerto con l'Organismo di Vigilanza, in sede di risk-assessment per la definizione di un eventuale Piano Annuale di Audit;
- Con interventi mirati in caso di:
    - Specifica richiesta formulata da parte degli altri organi di controllo della Società;

- In caso di non conformità derivanti dal flusso informativo correntemente operante nell'ambito del Modello.

L'Organismo di Vigilanza, utilizza come strumenti di controllo e azione anche quelli propri del Sistema qualità quali le non conformità, le azioni correttive e preventive, i piani di attività quali il piano di formazione e il programma di audit, il riesame della direzione e il rapporto di adeguatezza del sistema.

5.5. Flussi informativi

All'Organismo di Vigilanza devono essere trasmessi e tenuti costantemente aggiornati i documenti afferenti al sistema di procure e deleghe in vigore presso la Società

Allo stesso tempo, dovrà essere portata a conoscenza dell'Organismo di Vigilanza qualunque informazione, di qualsiasi tipo, che sia giudicata attinente all'attuazione del Modello nelle aree di attività a rischio così come individuate nel Modello.

L'obbligo riguarda principalmente le risultanze delle attività poste in essere dalla Società, nonché le atipicità e le anomalie riscontrate.

A tale riguardo valgono le seguenti prescrizioni:

- Devono essere raccolte le segnalazioni relative a possibili ipotesi di commissione di reati previsti dal Decreto o, comunque, di condotte non in linea con le regole di condotta adottate dalla Società;
- L'Organismo di Vigilanza valuterà le segnalazioni ricevute e adotterà i provvedimenti conseguenti, dopo aver ascoltato, se ritenuto opportuno, l'autore della segnalazione ed il responsabile della presunta violazione;
- Le segnalazioni potranno essere effettuate in forma scritta ed avere ad oggetto ogni violazione o sospetto di violazione del Modello e delle procedure aziendali adottate. L'Organismo di Vigilanza agirà in modo da garantire i soggetti segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando, altresì, l'assoluta riservatezza dell'identità del segnalante.

Oltre a ciò, devono essere necessariamente trasmesse all'Organismo di Vigilanza tutte le informazioni che presentino elementi rilevanti in relazione all'attività di vigilanza, come ad esempio:

- I provvedimenti o le notizie provenienti da organi di polizia o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini per i reati di cui al Decreto;
- Tutte le richieste di assistenza legale effettuate dalla Società;
- L'eventuale richiesta per la concessione di fondi pubblici in gestione o per l'ottenimento di forme di finanziamento dei fondi già in gestione;
- Le notizie relative all'attuazione, a tutti i livelli aziendali, del Modello organizzativo con evidenza dei procedimenti disciplinari intrapresi e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti.

Relativamente agli obblighi di informativa valgono al riguardo le seguenti prescrizioni:

- Devono essere raccolte tutte le segnalazioni relative alla commissione di reati previsti dal Decreto ed a comportamenti non in linea con le regole di condotta adottate;
- L'afflusso di segnalazioni deve essere canalizzato verso l'Organismo di Vigilanza della Società;

- L’Organismo di Vigilanza, valutate le segnalazioni ricevute, sentite le parti coinvolte (autore della segnalazione e presunto responsabile della violazione), determinerà i provvedimenti del caso;
- Le segnalazioni dovranno essere formalizzate per iscritto ed inoltrate anche attraverso posta elettronica alla casella a ciò specificatamente dedicata;
- Le stesse dovranno riguardare ogni violazione o sospetto di violazione del Modello.

Spetta all’Organismo di Vigilanza il compito di garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell’identità del segnalante e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Il materiale raccolto dall’Organismo di Vigilanza verrà conservato per 10 anni.

PARTE SESTA

INFORMAZIONE E FORMAZIONE

6.1. Informazione, formazione ed aggiornamento

Al fine di promuovere una cultura di impresa ispirata al rispetto della legalità e della trasparenza, PTS assicura l'ampia divulgazione del Modello e l'effettiva conoscenza dello stesso da parte di chi è tenuto a rispettarlo.

Una copia del Modello - nonché una copia di ogni intervenuta modifica e aggiornamento - è consegnata, oltre che al Consiglio di Amministrazione all'Organismo di Vigilanza, a ciascun dipendente ed a ciascun soggetto tenuto a rispettare le prescrizioni del Modello.

Una copia del Modello, Parte generale, e del Codice Etico e di Comportamento sono inseriti, in formato elettronico nel server aziendale, al fine di consentire ai dipendenti una consultazione giornaliera, e pubblicata sul sito della Società al fine di renderlo disponibile a tutte le parti interessate.

Prima dell'entrata in servizio i dipendenti neoassunti riceveranno una copia del Modello.

L'adozione del Modello e le sue successive modifiche ed integrazioni, sono portate a conoscenza di tutti i soggetti con i quali la Società intrattiene rapporti d'affari rilevanti.

PTS predispone, ogni anno, un piano di interventi formativi per i propri dipendenti e per le figure apicali al fine della completa acquisizione dei contenuti del Modello.

L'attività di formazione, finalizzata a diffondere la conoscenza della normativa di cui al D.L.gs. 231/2001 e successive modifiche, potrà essere differenziata per una maggiore efficacia nei contenuti e nelle modalità di attuazione in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui questi operano, dello svolgimento da parte degli stessi di funzioni di rappresentanza della Società e dell'attribuzione di eventuali poteri.

Tutti i programmi di formazione hanno un contenuto minimo comune consistente nell'illustrazione dei principi del D. L.gs. 231/2001, degli elementi costitutivi il Modello, delle singole fattispecie di reato previste dal D. L.gs. 231/2001 e dei comportamenti considerati sensibili in relazione al compimento dei sopracitati 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 e alle mansioni dei soggetti destinatari del programma stesso.

La formazione viene erogata secondo le scadenze che saranno indicate in un apposito programma ed in ogni caso a seguito di modifiche normative al regime della responsabilità degli enti ed a seguito di aggiornamenti rilevanti dei contenuti del Modello.

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

PARTE SETTIMA

DESTINATARI E CAMPO DI APPLICAZIONE

Il Modello comprende tutti i processi e le attività svolti dalla Società ed i Destinatari sono individuati nei componenti degli Organi sociali, in coloro che svolgono funzioni di gestione, amministrazione, direzione o controllo della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nei dirigenti e nei dipendenti della Società ed in generale in quanti si trovino ad operare sotto la direzione e/o vigilanza delle persone suindicate (tutti detti collettivamente "i Destinatari").

I principi e gli standard di controllo contenuti nel Modello si applicano altresì, nei limiti del rapporto contrattuale in essere, a coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa o sono comunque legati alla Società da rapporti giuridici rilevanti: tali Soggetti per effetto di apposite clausole contrattuali si impegnano a tenere, nell'ambito dei rapporti istituiti con la Società, comportamenti corretti e rispettosi delle disposizioni normative vigenti e comunque idonei a prevenire la commissione, anche tentata, dei reati in relazione ai quali si applicano le sanzioni previste nel Decreto.

PARTE OTTAVA

PROCEDURA DI ADOZIONE DEL MODELLO

Essendo il Modello un “atto di emanazione dell’organo dirigente”, in conformità con la disposizione di cui all’articolo 6, comma I, lettera a) del Decreto, le successive modifiche ed integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di PTS.

Le modifiche e/o le integrazioni al Modello che non presuppongono la necessità di attività di risk assessment possono essere promosse dall’Organismo di Vigilanza della Società, che ne darà successiva informazione al Consiglio di Amministrazione il quale ne disporrà l’approvazione.

L’efficacia del Modello Organizzativo approvato dal C.d.A. di PTS è condizionata all’approvazione del nuovo Organigramma organizzativo da parte di AdSP e alla nomina del O.d.V.

PARTE NONA

IL SISTEMA DISCIPLINARE

9.1. Principi generali

L'effettività del Modello è legata anche all'adeguatezza del sistema disciplinare e sanzionatorio, che presiede all'effettivo rispetto delle regole di condotta e, in generale, delle procedure e dei regolamenti interni.

L'applicazione di sanzioni disciplinari per violazione delle regole di condotta ed inosservanza delle disposizioni aziendali è indipendente dal giudizio penale e dal suo esito, in quanto tali normative sono assunte dalla Società in piena autonomia a prescindere dal carattere di illecito penale che la condotta possa configurare.

La sanzione è commisurata alla gravità dell'infrazione ed alla eventuale reiterazione della stessa; della recidività si tiene altresì conto anche ai fini della comminazione della sanzione.

Una errata interpretazione dei principi e delle regole stabiliti dal Modello da parte del soggetto sottoposto a procedimento può costituire esimente soltanto nei casi di comportamenti tenuti in buona fede, in cui i vincoli posti dal Modello dovessero eccedere i limiti di approfondimento richiesti ad una persona di buona diligenza con riferimento alla specifica mansione svolta.

All'Organismo di Vigilanza viene data comunicazione dell'apertura di ogni procedimento disciplinare e di ogni provvedimento di archiviazione e di sanzione inerente i procedimenti di cui al presente capitolo.

Nessun provvedimento disciplinare per violazione delle disposizioni del Modello nei confronti di qualsivoglia soggetto può essere adottato senza la preventiva consultazione dell'Organismo di Vigilanza.

9.2. Sanzioni per i lavoratori subordinati cui si applicano i Contratti Collettivi Nazionali di Lavoro

Ai lavoratori subordinati si applicano le sanzioni previste nei rispettivi CCNL di categoria, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori.

In applicazione delle norme relative alla disciplina del lavoro contenute nei vigenti CCNL, si prevede che:

1. incorre nei provvedimenti di richiamo verbale, ammonizione scritta, multa (non superiore a 3 ore della retribuzione base), sospensione dal lavoro e dalla retribuzione (fino a un massimo di 3 giorni) il lavoratore che violi le procedure interne previste dal Modello (ad esempio, che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.) o comunque adotti, nello svolgimento di attività nell'ambito di Processi Sensibili, un comportamento non conforme alle prescrizioni del Modello;

2. incorre nel provvedimento di licenziamento per mancanze il lavoratore che, nell'espletamento dei Processi Sensibili:

a) compia atti non conformi alle prescrizioni del Modello e diretti in modo univoco al compimento di un reato sanzionato dal D. L.gs. 231/2001, ravvisandosi in tale comportamento un'infrazione alla disciplina e ai doveri d'ufficio così grave da non consentire la prosecuzione nemmeno provvisoria del rapporto di lavoro, o,

b) abbia riportato condanna passata in giudicato per uno dei reati previsti nel Decreto.

Prima dell'adozione di qualsiasi provvedimento disciplinare nei confronti del lavoratore a questi sarà contestato l'addebito e lo stesso sarà sentito a sua difesa.

Ad eccezione del richiamo verbale, tutte le contestazioni avvengono per iscritto e i provvedimenti disciplinari non potranno essere applicati prima che siano trascorsi 5 giorni nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

L'adozione del provvedimento è motivata e comunicata per iscritto.

La contestazione delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano, nei limiti della competenza, nelle attribuzioni dei soggetti ai quali vengono dal vertice aziendale conferiti i relativi poteri.

9.3. Misure nei confronti dei dirigenti

Per i dirigenti, valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le infrazioni di maggiori gravità, così come individuate dal presente sistema disciplinare, la Società potrà addivenire al licenziamento del dirigente autore dell'infrazione.

9.4. Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte di taluno dei membri del Consiglio di Amministrazione, l'Organismo di Vigilanza ne darà immediata informazione al Consiglio di Amministrazione ed al Collegio Sindacale, i quali adotteranno i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'assemblea dei soci con l'eventuale proposta di revoca dalla carica. Le relative comunicazioni saranno indirizzate direttamente a tutti i componenti del Consiglio di Amministrazione, al Presidente del Collegio Sindacale ed ai sindaci effettivi.

9.5. Misure nei confronti dei Sindaci

In caso di violazione del Modello da parte del Sindaco o di adozione, nell'esercizio delle proprie attribuzioni, di provvedimenti che contrastino con le disposizioni o principi del Modello, l'Organismo di Vigilanza ne darà immediata informazione al Consiglio di Amministrazione, il quale adotterà i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'assemblea dei soci con la proposta di eventuale revoca dalla carica. Le relative comunicazioni saranno indirizzate direttamente a tutti i componenti del Consiglio di Amministrazione.

9.6. Misure nei confronti dell'Organismo di Vigilanza

In caso di violazione del presente Modello da parte dell'Organismo di Vigilanza uno qualsiasi tra i Sindaci o tra gli Amministratori, informerà immediatamente il Collegio Sindacale ed il Consiglio di Amministrazione: tali organi, previa contestazione della violazione e concessione degli adeguati strumenti di difesa,

prenderanno gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico all'Organismo di Vigilanza che abbia violato il Modello e la conseguente nomina di un nuovo Organismo di Vigilanza.

9.7. Misure nei confronti di Consulenti e Partner/Fornitori

La commissione dei reati di cui al D.L.gs. 231/2001 da parte di Consulenti o di Partner/Fornitori, così come ogni violazione da parte degli stessi delle regole di cui al Modello e del Codice Etico, comporta, per PTS che con gli stessi intrattiene rapporti, l'obbligo di azionare tutti gli strumenti contrattuali e di legge a disposizione per la tutela dei diritti della Società, ivi compresi ove del caso la risoluzione del contratto ed il risarcimento dei danni.

PARTE DECIMA

GESTIONE DELLE SEGNALAZIONI -WHISTLEBLOWING (L. 30.11.2017 n. 179)

10.1. Premessa

Per "whistleblowing" (di seguito "segnalazione") si intende qualsiasi segnalazione riguardante condotte anche omissive non conformi a leggi e regolamenti, comunque applicabili ad PTS, nonché al sistema di regole e procedure vigenti in PTS, tra le quali a titolo esemplificativo ma non esaustivo: il Codice Etico, il presente Modello Organizzativo.

il whistleblowing è stato oggetto di intervento legislativo a livello di D. Lgs 231/01 sulla responsabilità amministrativa dell'ente (Legge 30 novembre 2017, n 179 "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" che, all'articolo 2, ha previsto l'integrazione dell'articolo 6 del D.Lgs 231/01). In particolare, la previsione normativa si applica agli enti che hanno adottato un Modello Organizzativo 231 e si riferisce alle segnalazioni circostanziate di condotte illecite rilevanti ai sensi del decreto 231 o di violazioni del suddetto Modello. La normativa prevede, tra l'altro, il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante, in quanto lavoratore dipendente dell'ente, per motivi collegati, direttamente o indirettamente, alla segnalazione.

10.2. Il ruolo dell'Organismo di Vigilanza

Al fine di consentire l'attuazione delle disposizioni di cui all'art. 6, comma 2-bis, lettera a), del D.Lgs. 231/2001, valgono le seguenti prescrizioni:

- i soggetti in posizione apicale o sottoposti ad altrui direzione, ovvero coloro che a qualsiasi titolo collaborano o interagiscono con l'ente sono tenuti a trasmettere direttamente all'Organismo di Vigilanza, mediante una comunicazione in forma scritta da inviare all'indirizzo di posta ordinaria a "alla C.A. Organismo di Vigilanza di Porto di Trieste Servizi S.r.l., Via Karl Von Bruck n. 3 - 34122 Trieste (Italy)" o tramite e-mail a odv@portoditriesteservizi.it, eventuali segnalazioni circostanziate di condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o di violazioni del Modello di cui sono venuti a conoscenza in ragione delle funzioni che svolgono nell'ambito dell'Ente;
- ricevute le segnalazioni, l'Organismo di Vigilanza raccoglie tutte le ulteriori informazioni ritenute necessarie per una corretta e completa valutazione della segnalazione, anche avvalendosi della collaborazione di tutti i soggetti destinatari degli obblighi d'informazione di PTS;
- in nessun caso, l'Organismo di Vigilanza potrà tener conto di segnalazioni anonime. Le stesse potranno essere prese in considerazione solo ove risultino adeguatamente circostanziate, precise ossia in grado di far emergere fatti potenzialmente lesivi dell'interesse della Società tali da consentire l'apertura di un'istruttoria;
- l'Organismo di Vigilanza non è gravato dall'obbligo di verificare puntualmente e sistematicamente tutti i fenomeni potenzialmente sospetti o illeciti sottoposti alla sua attenzione. Infatti, la valutazione degli specifici casi nei quali sia opportuno procedere ad attivare verifiche ed interventi di maggiore dettaglio

è rimessa alla discrezionalità e responsabilità dell'Organismo stesso, che non è tenuto a prendere in considerazione le segnalazioni che appaiano in prima istanza irrilevanti, destituite di fondamento o non adeguatamente circostanziate sulla base di elementi di fatto.

Alla luce di quanto sopra esposto possono configurarsi due differenti scenari:

- l'Organismo di Vigilanza ritiene superfluo condurre indagini interne e procedere all'accertamento della segnalazione; in quanto caso il medesimo Organismo di Vigilanza dovrà, comunque, riferire della segnalazione pervenuta, nell'ambito dell'attività periodica di reporting, al Consiglio di Amministrazione;
- l'Organismo di Vigilanza ritiene necessario procedere all'accertamento della condotta illecita o della violazione del Modello di Organizzazione, Gestione e Controllo; in tal caso l'Organismo di Vigilanza ne dà comunicazione al Consiglio di Amministrazione ai fini dell'instaurazione del procedimento disciplinare nei confronti del prestatore di lavoro ai sensi dell'art. 7 dello Statuto dei Lavoratori e nel pieno rispetto del principio del contraddittorio tra le Parti, tenendo conto delle specificità dello status giuridico del soggetto nei cui confronti si procede (soggetto apicale, sottoposto ad altrui direzione o collaboratore dell'Ente).

In considerazione dell'imprescindibile coinvolgimento dell'Organismo di Vigilanza nel procedimento di irrogazione delle sanzioni disciplinari, all'esito della fase istruttoria questo è tenuto a formulare pareri non vincolanti in relazione alla tipologia e all'entità della sanzione da irrogare nel caso concreto.

In ogni caso, l'Organismo di Vigilanza raccoglie e conserva tutte le segnalazioni in un'apposita banca dati in formato telematico e/o cartaceo. I dati e le informazioni conservati nella banca dati possono essere messi a disposizione di soggetti esterni all'Organismo di Vigilanza previa autorizzazione dello stesso, salvo che l'accesso debba essere consentito ai sensi di legge.

L'Organismo di Vigilanza definisce altresì, con apposita disposizione interna, i criteri e le condizioni di accesso alla banca dati, nonché quelli di conservazione e protezione dei dati e delle informazioni nel rispetto della normativa vigente.

Al fine di garantire la riservatezza sull'identità del segnalante, l'Organismo di Vigilanza e i soggetti designati a suo supporto si impegnano a mantenere il più stretto riserbo sulle segnalazioni e a non divulgare alcuna informazione che abbiano appreso in occasione dell'esercizio delle proprie funzioni. In particolare, l'Organismo di Vigilanza agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione o penalizzazione e, più in generale, contro qualsiasi conseguenza negativa derivante dalle stesse, assicurando la massima riservatezza circa l'identità del segnalante. In ogni caso, sono fatti salvi gli obblighi imposti dalla legge e la tutela dei diritti dell'Ente o dei soggetti accusati erroneamente e/o in mala fede e/o calunniosamente.

Le suddette disposizioni si applicano esclusivamente alle segnalazioni aventi ad oggetto le violazioni del Modello adottato dalla Società.

10.3. Nullità delle misure ritorsive e discriminatorie adottate nei confronti del segnalante.

L'autore della segnalazione di illecito ha la possibilità di denunciare l'adozione di misure discriminatorie nei propri confronti all'Ispettorato Nazionale del Lavoro, oltre alla facoltà riconosciuta al segnalante medesimo

di rivolgersi direttamente alla propria organizzazione sindacale di riferimento, ex art. 6, comma 2 ter del Decreto.

È, in ogni caso, stabilita la nullità del licenziamento ritorsivo o discriminatorio, del mutamento di mansioni ai sensi dell'art. 2103 c.c. ("Prestazione del lavoro"), nonché di qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del soggetto segnalante.

La norma grava inoltre il datore di lavoro dell'onere di dimostrare - in occasione di controversie legate all'irrogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti o alla sottoposizione del segnalante ad altra misura organizzativa successiva alla presentazione della segnalazione avente effetti negativi, diretti o indiretti, sulla condizione di lavoro - che tali misure sono fondate su ragioni estranee alla segnalazione stessa (cd. "inversione dell'onere della prova a favore del segnalante").

10.4. Perdita delle tutele garantite dalla legge in caso di malafede del segnalante

Le tutele accordate ai soggetti in posizione apicale, ai sottoposti ad altrui direzione, nonché a coloro che collaborano con l'Ente vengono meno qualora sia accertata, anche soltanto con sentenza di primo grado, la responsabilità penale dell'autore della segnalazione per i reati di calunnia, diffamazione o per altri reati in concreto riconducibili alla falsità della denuncia. Parimenti, le tutele a favore del segnalante non sono garantite nel caso in cui quest'ultimo sia ritenuto responsabile in sede civile per aver sporto segnalazioni infondate, con dolo o colpa grave.

PARTE SPECIALE

PARTE UNDICESIMA

FINALITÁ E STRUTTURA DELLA PARTE SPECIALE

11.1. Finalità della Parte Speciale

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

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

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

Il Consiglio di Amministrazione nel definire tale documento, a ulteriore conferma della volontà aziendale di operare secondo principi "etici" così come già contemplati nella propria regolamentazione interna e specificamente nel "Codice Etico e di comportamento" nella versione pubblicata sul sito aziendale, intende sensibilizzare tutto il personale a mantenere comportamenti corretti e idonei a prevenire la commissioni di reati.

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

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

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

- Modello;
- Codice Etico e di Comportamento;
- Procedure e disposizioni;
- Procure e deleghe;
- Le "schede di servizio" definite con AdSP, per quanto di rispettiva competenza di ciascun esponente aziendale
- Ordini di servizio;
- Comunicazioni organizzative;
- Sistemi di gestione delle problematiche di sicurezza;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

Altrettanto in via generale, a tutto il personale dell'azienda è fatto divieto di:

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

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

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

11.2. Struttura della Parte Speciale

Il D. L.gs. 231/01, all'Articolo 6, Comma 2, indica le caratteristiche essenziali per la costruzione di un modello di organizzazione, gestione e controllo; la lettera a), in particolare, si riferisce espressamente ad un tipico sistema di gestione dei rischi.

La norma qualifica il processo di "identificazione dei rischi" come l'analisi del contesto aziendale per evidenziare dove (ovvero in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D. L.gs. 231/01.

Attraverso la valutazione della situazione aziendale, in relazione ai possibili reati, PTS ha definito i rischi ed è stata verificata l'eventuale necessità di predisporre strumenti di controllo aggiuntivi rispetto a quelli già presenti.

PTS, in particolare, ha effettuato una dettagliata analisi dei rischi connessi alle diverse fasi delle attività aziendali, verificando ed individuando le aree che risultano interessate dalle potenziali casistiche di reato.

Successivamente sono state evidenziate le tipologie di reato connesse alle specifiche attività, individuando le risorse che, potendo essere coinvolte nella gestione del rischio, devono essere oggetto del sistema di controllo pianificato.

Per ogni tipologia di reato/attività, è stato assegnato un valore di "accettabilità" del rischio in base al livello di efficacia del sistema di controllo messo in atto per la gestione della specifica attività.

L'applicazione della procedura di identificazione e valutazione dei rischi è necessaria durante:

- La fase iniziale dell'implementazione del Modello, in conformità con il D. L.gs. 231/01, in quanto costituisce la base per la definizione degli obiettivi e dei programmi e comunque prima di ogni riesame del sistema al fine di garantire un aggiornamento sistematico della valutazione dei rischi;
- Ogni qual volta avvenga una variazione di processo, di prodotto o del sito o del contesto in cui la Società opera quali ad esempio modifiche del quadro legislativo di riferimento;
- Ad ogni riesame di sistema.

11.3. Principi ispiratori

Normalmente il sistema delle deleghe e di attribuzione dei poteri costituisce la parte essenziale e sostanziale del Modello 231. Tanto vale per le realtà aziendali articolate e complesse ma non per quelle che - pur inserite in un contesto di grande complessità e rilevanza - presentano un livello organizzativo, strutturalmente, ridotto al minimo.

Sul punto, si è già evidenziato nella Parte Generale del Modello (v. punto 4.2) come la recente trasformazione aziendale, unitamente all'affidamento di sempre più rilevanti e consistenti attività operative da parte di AdSP, in conseguenza delle aumentate aree di competenza di quest'ultima, hanno comportato la necessità per PTS di implementare una struttura sempre più complessa in grado di soddisfare le molteplici e diverse esigenze rappresentate dal Socio Unico.

L'aumento delle attività affidate e il relativo incremento del personale hanno indotto la necessità di elaborare una nuova ripartizione dei compiti e delle attività ed una conseguente concreta segregazione dei compiti e delle responsabilità.

PTS si trova, al momento della redazione del presente Modello organizzativo, in una fase di transizione tra la struttura aziendale precedente, caratterizzata dal rapporto diretto tra il centro decisionale e gli addetti operativi e la nuova organizzazione ancora in fase di implementazione.

Per le dette ragioni PTS ritiene necessario concentrarsi sulle attività di controllo, anche preventivo, e di monitoraggio che sono svolte dall'Organo di Amministrazione con il supporto di soggetti indipendenti esterni alla organizzazione aziendale (Collegio Sindacale, Organismo di Vigilanza e Controllo Analogo di AdSP).

La concreta implementazione della nuova organizzazione aziendale si sta attuando attraverso la formalizzazione di una serie di deleghe ai singoli responsabili di settore e con l'attribuzione all'organo dirigenziale delle attività di coordinamento delle attività aziendali. Tanto permette l'identificazione di diversi livelli autorizzativi rappresentativi dei poteri e delle responsabilità riferibili alle mansioni attribuite e alle posizioni ricoperte nell'ambito della struttura organizzativa e, conseguentemente, una riduzione del rischio di commissione dei reati previsti nel Decreto.

Con la definitiva implementazione della nuova struttura organizzativa il *management* della Società potrà focalizzare sulle attività *core* e cioè, in estrema sintesi:

- La funzione manutentiva di tutte le reti e infrastrutture del Porto (siano esse edili, meccaniche, elettriche, di *security* e di *safety*);
- La funzione di gestione della viabilità interna e retro-portuale (incluso cioè il flusso in arrivo con i collegamenti e le aree parcheggio esterne nell'ambito di competenza della *Authority*);
- La gestione della segnaletica stradale nell'area portuale;
- Gli altri numerosi interventi *"spot"* non programmabili svolti sia in ambito portuale che retro-portuale, supportando l'AdSP in tutte le aree di competenza di quest'ultima.

11.4. Il sistema dei poteri e delle deleghe

Nell'ambito della predetta fase transitoria e nei limiti della sua concreta implementazione PTS attua il principio della segregazione delle responsabilità in linea con quanto consentito dalla normativa vigente.

Il socio unico (AdSP) esercita il Controllo Analogo nei confronti di PTS in quanto propria *Società in house providing*. A tal fine PTS invia a AdSP le relazioni semestrali per i controlli previsti da Statuto.

Al Consiglio di Amministrazione di PTS sono riconosciuti, tutti i poteri di ordinaria e straordinaria amministrazione ad esclusione solo di quelli riservati all'Assemblea dalla legge e dei poteri autorizzativi riconosciuti al Socio Unico, non risultando infatti da Statuto altre limitazioni.

In base all'assemblea straordinaria del 14 giugno 2018, risulta nominato un Consiglio di Amministrazione composto dal Presidente e legale rappresentante e da due consiglieri senza deleghe.

I poteri di firma e di rappresentanza possono essere rilasciati ai dipendenti o, eventualmente, a terzi dai legali rappresentanti aziendali nell'ambito delle rispettive competenze e dei relativi poteri.

Contestualmente all'approvazione del presente Modello organizzativo il C.d.A. ha approvato le deleghe in materia di sicurezza e ambientale.

PARTE DODICESIMA

ANALISI E MAPPA DEI RISCHI

12.1. Premessa

Come anticipato, preliminarmente all'implementazione del Modello Organizzativo 231, è stata effettuata una mappatura dei rischi come previsto dal D.L.gs n. 231/2001.

La rilevazione è stata impostata attraverso un processo di autovalutazione, effettuato dai responsabili addetti alle aree "sensibili", identificati, nello specifico, nella persona del Direttore Generale e della Responsabile anticorruzione e trasparenza.

Il processo di autovalutazione è stato effettuato tenendo in debita considerazione la natura del socio unico e delle finalità delle società in house, rilevante per la normativa in oggetto.

12.2. Metodologia di lavoro

Per effettuare una mappatura dei rischi, si è operato, come detto, con la tecnica dell'autovalutazione che ha coinvolto la direzione aziendale e tutti gli addetti. Il metodo adottato ha consentito di identificare una serie di "ambiti" e processi di particolare interesse per la prevenzione e la tempestiva individuazione di comportamenti e prassi che possono determinare la commissione di reati "231".

L'output finale, il cui principale elemento è costituito dalla mappa dei rischi, è sostanzialmente costruito sulla base di una valutazione e da successivi approfondimenti dei processi considerati sensibili ai fini del D. L.gs. 231/2001. Lo scopo è, appunto, quello di indicare gli "ambiti" che vanno comunque sempre tenuti sotto monitoraggio attivo. Pertanto, sono stati identificati i processi e le attività "sensibili" nei quali è più opportuno che siano presenti specifici strumenti di controllo (procedure, indicatori di anomalie, etc.) idonei a prevenire la commissione di illeciti "231" ed inoltre sono state individuate le funzioni eventualmente più esposte ai reati "231".

12.3. Individuazione dei processi aziendali di interesse ai fini del D. L.gs. 231/2001

Si riporta di seguito l'elenco dei processi aziendali selezionati, in quanto impattanti da tematiche riferibili al D. L.gs. 231. Anche in questo caso, si è assegnato un profilo di rischio potenziale che dipende da fattori quali la complessità dell'area, la numerosità dei soggetti che svolgono la specifica attività, la "visibilità" del loro operato (dipendenti o terzi), etc.

PROCESSO A RISCHIO REATO	Prevenzione, protezione e formazione del personale
PROCESSO A RISCHIO REATO	Acquisti di beni e servizi
PROCESSO A RISCHIO REATO	Gestione delle attività amministrative e redazione del bilancio

Sono stati individuati anche processi strumentali, nel senso che pur non essendo direttamente esposti al rischio reati si potrebbero, all'interno del proprio ambito, creare le condizioni strumentali per la commissione

di reati previsti dal D. L.gs. 231/01 (Esempio: finanza dispositiva, selezione ed assunzione di personale, gestione delle consulenze, gestione degli omaggi etc.,)

PROCESSO STRUMENTALE	Disciplina Privacy
PROCESSO STRUMENTALE	Selezione e assunzione di personale
PROCESSO STRUMENTALE	Smaltimento rifiuti

Pertanto, le tipologie di reati di interesse per la Società sono risultate le seguenti:

- Reati commessi nei rapporti con la P.A.;
- Reati societari;
- Reati di ricettazione, riciclaggio, impiego di denaro, beni o altra utilità di provenienza illecita, autoriciclaggio;
- Reati informatici e trattamento illecito dei dati;
- Reati ambientali

Con riferimento alla materia della sicurezza sul lavoro la Società ha implementato un sistema di controlli coerente con i requisiti previsti dall'art. 30 D. L.gs. 81/2008 e s.m.i. secondo le indicazioni della Circolare del Ministero del Lavoro e delle politiche sociali del 11 luglio 2011. Ha pertanto nominato un RSPP esterno che pianifica e di fatto esegue controlli ciclici.

Non sono stati denunciati casi gravi, né significativi, di infortuni sul lavoro negli ultimi tre anni. Per quanto riguarda quindi l'identificazione delle attività a rischio reato, le procedure di controllo, la valutazione dei rischi ed azioni di miglioramento, si fa rinvio ai controlli ed al DVR per evitare inutili ripetizioni. Resta naturalmente opportuno e necessario un costante coordinamento tra RSPP e ODV (oltre al coordinamento già posto in essere autonomamente da parte dell'RSPP e i vari attori aziendali).

Non è stato, poi, considerato significativo il rischio di commissione dei reati di mutilazione degli organi genitali femminili previsti dall'art. 25-quater.1 del Decreto, trattandosi di condotte che non potrebbero essere compiute nell'ambito delle attività aziendali nell'interesse e/o a vantaggio della Società.

L'eventuale impiego di cittadini stranieri con permesso di soggiorno irregolare è di fatto impedito dai controlli sulla documentazione richiesta ai nuovi assunti in fase di formalizzazione del rapporto di lavoro, mentre apposite clausole contrattuali nei rapporti con fornitori e partner prevedono divieti di cessione del contratto e di subappalto, salvi i casi di espressa autorizzazione ed impongono ai fornitori di utilizzare solo manodopera regolare nel rispetto delle disposizioni normative vigenti.

Il rischio di realizzazione di condotte corruttive nei confronti di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori è stato ravvisato con riferimento alle attività finalizzate ai "Rapporti commerciali di acquisto beni/servizi ivi inclusi servizi di consulenza e marketing (c.d. ciclo passivo)"–nonché con riferimento alle aree ed attività sensibili c.d. "strumentali", cioè tutte quelle attività (quali ad esempio l'area di rischio "Gestione dei pagamenti") che potrebbero fornire il denaro o altra utilità richiesti dall'art. 2635 c.c. come prezzo della corruzione tra privati: oltre ai controlli descritti in tali parti del Modello. PTS aveva già adottato un proprio Codice Etico e di comportamento che viene modificato per integrarlo e adeguarlo alla normativa sopravvenuto al presente Modello organizzativo. PTS promuove la sensibilizzazione di tutti i dipendenti al rispetto dei principi e dei valori contenuti nel Codice Etico e del presente Modello Organizzativo nell'ambito delle iniziative di formazione ed informazione.

12.4. Mappa dei rischi "231" e valutazione

Di seguito si riporta una tabella in cui vengono riassunti i risultati della valutazione dei rischi.

PROCESSI/ ATTIVITÀ	Funzioni coinvolte	Reati contro la P.A.	Reati societari	Reati informatici	Ricettazione e riciclaggio	Reati ambientali
Gestione rapporti con la P.A.	CDA DG AMM	B	BN	BN	NP	NP
Manutenzione: Infrastrutture	CDA DG RF	BN	NP	BN	NP	B
Manutenzione: continuità operativa	CDA DG RF	BN	NP	BN	NP	B
Servizi	CDA DG RF	BN	NP	BN	NP	B
Segnaletica	CDA DG RF	BN	NP	BN	NP	B
Gestione attività amministrative e redazione del bilancio	CDA DG AMM	B	B	BN	B	B
Finanza dispositiva Tesoreria	CDA DG AMM	M	B	BN	B	NP
Acquisti di beni e servizi	CDA DG AMM UA	B	B	BN	NP	NP
Selezione ed assunzione del personale	CDA AMM RF	B	B	BN	NP	NP
Consulenze e prestazioni professionali	CDA RF	B	B	BN	NP	NP

LEGENDA

CDA	Consiglio di Amministrazione	NP	Rischio non presente
UA	Ufficio acquisti	BN	Rischio basso o nullo
AMM	Amministrazione	B	Rischio basso
RF	Responsabile di funzione	M	Rischio medio
DG	Direttore Generale	A	Rischio alto

Con riferimento ad ognuno dei settori e delle aree ritenute più specificatamente a rischio, sono state elaborate le ipotesi di comportamenti delittuosi che potrebbero essere poste in essere nell'ambito del processo/attività aziendale di riferimento (occasione, finalità e modalità di esecuzione del comportamento illecito), accompagnate dalle identificazioni dei processi contenenti i controlli finalizzati alla mitigazione del rischio di comportamenti illeciti.

Rientrano tra le misure di prevenzione già esistenti i principi comportamentali più generali inseriti nel Codice Etico e nel presente Modello.

Nello specifico, sono state individuate le attività / processi che determinano l'esistenza di contatti diretti o indiretti (tramite documenti, dati, informazioni, dichiarazioni, etc.) con le strutture / persone della Pubblica Amministrazione (reati contro la P.A.) o con gli stakeholders a cui sono indirizzate le informazioni di natura economica e finanziaria (reati societari), nel cui ambito, a seguito di determinate azioni, possono potenzialmente verificarsi comportamenti contrari ai disposti di Legge.

12.5. Specifiche circa i delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli Enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del d.lgs. 231/2001).

L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto. Si tratta di un'ipotesi particolare del c.d. "recesso attivo", previsto dall'art. 56, comma 4, c.p.

12.6. Considerazioni finali

Le considerazioni che supportano l'opinione del livello di rischio formulato nel presente documento, sono comunque basate sul presupposto che le procedure e i controlli vengano effettivamente applicati.

Nelle aree di rischio individuate, sono elencati gli illeciti penali che potrebbero verificarsi qualora venissero aggirate le procedure ed i controlli aziendali.

Al riguardo si rileva che:

- PTS è adeguatamente strutturata in termini di prassi / procedure, tenuto conto dell'introduzione del Regolamento per il reclutamento del personale e del Regolamento acquisti, fondamentali sia per il funzionamento che per il proprio *core business*.
- Il sistema organizzativo, il sistema di gestione ISO 9001 – 2015, la certificazione "FGAS" ed il sistema di deleghe e procure, costituiscono un impianto già valido ad integrare le eventuali ulteriori attività di monitoraggio e controllo, nei rispettivi ambiti;
- L'opportuna implementazione del sistema di pianificazione e reporting, del processo di controllo dei ricavi, dei costi e delle spese, dei sistemi di gestione 14001 (gestione ambientale) e 49001 (gestione sicurezza) determinerà nel breve termine un'ulteriore mitigazione dei rischi rilevanti ed efficientamento delle attività di monitoraggio;

- Il Direttore Generale svolge un ruolo attivo di indirizzo, gestione e controllo, ma l'effettivo inserimento della figura di "Direttore *Operation*", al momento solo indicata nell'organigramma ma non concretamente coperta consentirà al Direttore Generale di meglio focalizzarsi sulle proprie attività *core*;
- Nella storia della Società non risultano eventi contestati dalle pubbliche autorità che si riferiscono a tipologie di reato "231".

PARTE TREDICESIMA

REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

13.1. 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 di quei soggetti qualificati come "soggetti attivi" nei reati rilevanti ai fini del Decreto, ovvero di quei soggetti la cui qualifica è necessaria ad integrare fattispecie criminose previste nel Decreto.

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

13.2. 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. L.gs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

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

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

Venendo a quanto più specificamente di interesse, mette conto ricordare che "l'Autorità di sistema portuale del Mare Adriatico orientale", oltre ad essere Socio unico e titolare del controllo analogo nei confronti di PTS,

propria società in house, alla medesima eroga annualmente contributi in conto esercizio nel rispetto del Patto d'Intesa stipulato tra quella Autorità e la Società stessa e del Programma Operativo annuale approvato; soprattutto, come noto, il fatturato di PTS deve derivare e di fatto deriva per almeno l'80 per cento dai servizi resi a AdSP .

Considerato quindi che l'Autorità di sistema portuale è un ente pubblico non economico, sia pur dotato di autonomia amministrativa, di bilancio e finanziaria, assoggettato alla vigilanza del Ministero delle Infrastrutture, le condotte dei dipendenti della Società andranno considerate sotto il profilo della prevenzione dei reati commessi nei rapporti con la PA.

Si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose previste dal Decreto.

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

13.3. Pubblici Ufficiali

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

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

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

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

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

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

- Poteri deliberativi;
- Poteri autoritativi;
- Poteri certificativi

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

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

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

13.4. Incaricati di Pubblico Servizio

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

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

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

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

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

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

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

Sulla base di quanto sopra riportato, si potrebbe ritenere che l'elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di "incaricato di un pubblico servizio" è rappresentato, non dalla natura

giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

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

13.5. Le Società in house nella prospettiva del D. L.gs. 231/2001

I destinatari del Decreto sono individuati all' art. 1 che, al secondo e terzo comma, testualmente recita:

"2. Le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità.

"3. Non s i applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzione di rilievo costituzionale."

Dal tenore letterale della norma possono evincersi chiaramente gli intenti del Legislatore che, da un lato, utilizzando l' espressione "*enti*" piuttosto che "*persone giuridiche*" ricomprende nel novero dei soggetti passibili di responsabilità ex decreto 231 anche quelli privi di personalità giuridica; dall' altro lato emerge ancor più chiaramente la volontà di escludere dai destinatari di detta disciplina tutti quei soggetti giuridici che rivestono un ruolo di carattere pubblico: oltre allo Stato e gli enti pubblici territoriali (regioni, provincie, comuni) anche gli enti pubblici non economici e gli enti che svolgono funzioni di rilievo costituzionale.

Sin dalle prime applicazioni si sono posti dubbi sull' effettiva portata applicativa di quest' assunto, in particolare sul rilievo che la locuzione "*enti pubblici*" dovesse intendersi in maniera estensiva o restrittiva.

Un chiarimento è stato fornito dalla stessa legge delega n. 300/2000 che, all'art. 11, ha stabilito che il Decreto disciplina la responsabilità amministrativa delle "*persone giuridiche e delle società, associazioni od enti privi di personalità giuridica che non svolgono funzioni di rilievo costituzionale*"; e ancora, il comma 2 del medesimo articolo dispone che "*per persone giuridiche s'intendono gli enti forniti di personalità giuridica, eccettuati lo Stato e gli altri enti pubblici che esercitano pubblici poteri*".

Va da sé che, per logica conseguenza, il decreto legislativo avrebbe dovuto escludere anche le regioni, i comuni e le provincie. Ebbene, mentre non possono nutrirsi dubbi sull' esenzione dalla responsabilità per lo Stato e gli altri enti pubblici territoriali, l'espressione "*enti che esercitano pubblici poteri*" ha destato non pochi problemi interpretativi. In particolare, per quanto riguarda quegli enti che erogano un servizio pubblico e per le società partecipate da enti pubblici.

Quanto alla prima di queste categorie la questione è stata risolta dal legislatore delegato con la chiara esclusione degli enti che svolgono funzioni di rilievo costituzionale; così rimangono escluse dall' ambito di applicazione del decreto in commento le aziende ospedaliere, le scuole, le università, ma anche gli ordini o i collegi professionali.

Maggiori dubbi esegetici si sono posti, invece, per tutte gli enti che, pur svolgendo attività economica a scopo lucrativo, hanno in modo diretto o indiretto una presenza pubblica nella compagine sociale e che svolgono un'attività di pubblica utilità.

La dottrina prevalente ha ritenuto estendere l'applicabilità del Decreto anche a questi enti, ancorché aventi un carattere pubblico (seppur indiretto), in ragione del fatto che, comunque, gli stessi svolgono un'attività di

tipo economico- lucrativa; invece il decreto, assai chiaramente, esclude dai destinatari soltanto quei soggetti pubblici non economici.

Tale orientamento è stato confermato dalla Suprema Corte di Cassazione con le sentenze n. 28699/2010 e 234/2011 ove si è affermato un importante principio in forza del quale il D.lgs. n. 231 / 2001 è applicabile anche agli enti economici partecipati da soggetti pubblici.

Detto principio si fonda su un'interpretazione letterale della norma di cui all' art. 1 e, segnatamente, si basa sull' esclusione di quegli enti che, oltre allo stato e agli enti pubblici territoriali, svolgono attività di carattere non economico o di rilievo costituzionale. "*La ratio dell'esenzione è infatti quella di escludere dall' applicazione delle misure cautelari e delle sanzioni previste dal d. lgs. n. 231/ 2001 enti non solo pubblici, ma che svolgano funzioni non economiche, istituzionalmente rilevanti, sotto il profilo dell'assetto costituzionale dello Stato amministrazione*. *In questo caso, infatti, verrebbero in considerazione ragioni dirimenti che traggono la loro origine dalla necessità di evitare la sospensione di funzioni essenziali nel quadro degli equilibri dell'organizzazione costituzionale del Paese*" (Cass. Pen. n. 234/2011).

Sulla base del contributo offerto dalla Suprema Corte deve necessariamente leggersi in modo restrittivo la disposizione di cui al terzo comma dell'art. 1 D. lgs. n. 231/ 2001. Invero non ci sono ragioni di opportunità pubblica per escludere dal novero dei soggetti passibili di responsabilità amministrativa dipendente da reato le società partecipate da enti pubblici qualora questi svolgano attività di carattere economico. A conforto di una simile interpretazione è sufficiente ricordare che tra i reati presupposto del D. lgs. n. 231 /2001 vi sono i delitti di corruzione passiva del pubblico ufficiale e dell'incaricato di pubblico servizio, nonché di corruzione. In quest'ottica restrittiva la normativa de qua non risulterà, invece, applicabile agli enti, ancorché sotto forma di società di diritto comune, che svolgono attività di rilievo costituzionale, proprio in ragione della rilevanza costituzionale dell'attività svolta.

Chiarita la necessità, anche per le società a partecipazione pubblica e, maggior ragione, per le società *in house*, a ciò deve aggiungersi che la Legge n. 190/2012 prevede l'obbligo per le pubbliche amministrazioni di predisporre un piano triennale di prevenzione della corruzione al fine di prevenire il rischio di commissione dei suddetti reati (art. 1, comma 5).

La circolare n. 1 del 25 gennaio 2013 del Dipartimento della Funzione Pubblica, chiarisce che il concetto di corruzione, ai fini dell'ambito di applicazione della Legge 190/2012, deve essere inteso in senso lato, "*come comprensivo delle varie situazioni in cui, nel corso dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati*".

Dall'introduzione della Legge n. 190/2012 si è posto il problema del coordinamento del modello ex D. Lgs. 231/2001 con il Piano Triennale di Prevenzione della Corruzione.

Sul punto si è espressa l'Autorità Nazionale Anticorruzione che ha chiarito, con il Piano Nazionale Anticorruzione, che non vi è alcuna incompatibilità tra il modello 231 e il Piano Triennale per la Prevenzione della Corruzione (PTPC).

Nello specifico nel PNA si legge: "Gli enti pubblici economici e gli enti di diritto privato in controllo pubblico, di livello nazionale o regionale/locale sono tenuti ad introdurre e ad implementare adeguate misure organizzative e gestionali e per evitare inutili ridondanze qualora questi enti adottino già modelli di organizzazione e gestione del rischio sulla base del d. lgs. n. 231 del 2001 nella propria azione di prevenzione della corruzione possono fare perno su essi, ma estendendone l'ambito di applicazione non solo ai reati contro la pubblica amministrazione previsti dalla l. n. 231 del 2001 ma anche a tutti quelli considerati nella l. n. 190 del 2012, dal lato attivo e passivo, anche in relazione al tipo di attività svolto dall' ente (società strumentali/ società di interesse generale). Tali parti dei modelli di organizzazione e gestione, integrate a i

sensi della l. n. 190 del 2012 e denominate Piani di prevenzione della corruzione, debbono essere trasmessi alle amministrazioni pubbliche vigilanti ed essere pubblicati sul sito istituzionale".

Quanto al coordinamento tra la figura del Responsabile della Prevenzione della Corruzione ex L. n. 190 / 2012 e l'OdV ai sensi del D. lgs. n. 231/ 2001, si pone il problema della composizione dell'OdV atteso che i membri di quest'ultimo organo (non nel senso tecnico del termine) devono avere i requisiti di autonomia e indipendenza e, conseguentemente, privi di qualsiasi subordinazione con l'ente mentre il Responsabile della Prevenzione alla Corruzione (RPC) è un organo monocratico incardinato nel contesto organizzativo e dotato di compiti prettamente operativi. Ragioni pratiche e di opportunità inducono ad escludere la sovrapponibilità tra queste due figure che, comunque, devono necessariamente coordinare la loro relativa attività al fine di porre in essere un concreto ed effettivo contrasto alla commissione dei reati.

13.6. Le fattispecie di reato richiamate dal D. L.gs. 231/2001

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

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del d.lgs. n. 231/2001, si riporta, qui di seguito, una breve descrizione dei reati richiamati dagli art. 24 (Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico) e art.25 (concussione e corruzione) del D. L.gs. 231/01.

a. Peculato (Art. 314 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio che avendo per ragioni del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa se ne appropria.
La pena prevista per tale reato dall'art. 1. della legge n.69 del 27 maggio 2015 che ha modificato l'art. 314 c.p., è la reclusione da quattro a dieci anni e sei mesi.
Si applica invece la pena della reclusione da sei mesi a tre anni quando il colpevole ha agito al solo scopo di fare uso momentaneo della cosa e questa viene immediatamente restituita.

Esempio

Un pubblico ufficiale utilizza la carta di credito aziendale per ragioni private.

b. Malversazione a danno dello Stato o dell'Unione Europe (Art. 316 bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). La pena prevista per il reato in oggetto è la reclusione da sei mesi a quattro anni.
Per i dipendenti il reato in oggetto potrà configurarsi nell'ipotesi in cui le sovvenzioni siano erogate a favore della azienda perché ne fruisca direttamente ovvero perché si faccia tramite della loro distribuzione ai privati destinatari dell'erogazione.

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

Esempio

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

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

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

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

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

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

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

Esempio

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

d. *Truffa in danno dello Stato o di altro Ente Pubblico o dell'Unione Europea (Art. 640, comma 2, n. 1, c.p.)*

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

La pena prevista è quella della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro.

Esempio

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

e. *Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640 bis)*

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

La pena prevista è quella della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro.

Esempio

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

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

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

Tale reato è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a 1.032 euro ovvero, se il fatto è commesso a danno dello Stato o di un altro ente pubblico.

Se il fatto è commesso con abuso della qualità di operatore del sistema, con la reclusione da uno a cinque anni e con la multa da 309 euro a 1.549 euro.

Infine, se il fatto è commesso con furto o indebito utilizzo dell'identità digitale, in danno di uno o più soggetti, la pena è la reclusione da due a sei anni e la multa da 600 a 3000 euro.

Esempio

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

g. Concussione (Art. 317 c.p.)

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

La pena prevista per tale reato dall'art.3 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 317 c.p. è la reclusione da sei a dodici anni.

Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto, o allorquando la società svolga attività di incaricato di pubblico servizio (ad es. quando svolge l'attività volta alla riscossione tributi).

Esempio

Si consideri il caso di una società che partecipi ad una gara pubblica. In questo caso è possibile che i funzionari pubblici pongano in essere dei comportamenti concussivi in danno di terzi, per avvantaggiare la società che in ipotesi potrebbe concorrere con i funzionari pubblici per trarne beneficio e aggiudicarsi la gara.

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

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, riceve indebitamente per sé o per altri, denaro o altri vantaggi o ne accetta la promessa.

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

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

La pena prevista per tale reato dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 318 c.p. è la reclusione da uno a sei anni.

Esempio

Sindaco che agevola appalti in favore dei cari o agevola l'affidamento degli appalti in favore delle persone a lui più vicine.

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

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per omettere o ritardare un atto d'ufficio (determinando un vantaggio in favore dell'offerente), riceve indebitamente per sé o per altri, denaro o altri vantaggi o ne accetta la promessa.

La pena prevista per tale reato dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 319 c.p. è la reclusione da sei a dieci anni.

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

Esempio

Medico che favorisce la prescrizione e la vendita di medicinali di una determinata ditta farmaceutica ottenendo da questa denaro o altro per sé e per i suoi cari.

j. 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 abusando dei suoi poteri induce taluno a dare o a promettere per sé o per altri, denaro o altra utilità.

La pena prevista per tale reato dall'art.1 della legge n. 69 del 27 maggio 2015 che ha modificato l'art. 319 quater è la reclusione da sei a dieci anni e sei mesi.

Esempio

Un dirigente offre una somma di denaro ad un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo necessario per l'esercizio dell'attività della società.

k. Corruzione di persona incaricata di un Pubblico Servizio (Art. 320 c.p.)

Le disposizioni degli artt. 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

Le pene comunque sono ridotte in misura non superiore ad un terzo.

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

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

La pena prevista per tale reato dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 319 ter è la reclusione da sei a 12 anni.

Se dal fatto deriva la ingiusta condanna alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni. Se l'ingiusta condanna alla reclusione è superiore ai cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni.

Esempio

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

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

Le stesse pene previste dagli artt. 318,319,319 bis,319 ter,320 si applicano a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.

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

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

Tale reato è punito con le pene previste per i reati di cu agli artt. 318 e 319 c.p., ridotte di un terzo.

Esempio

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

o. Peculato, concussione, corruzione ed istigazione alla corruzione di membri degli organi e di funzioni della Comunità Europea e di Stati esteri (Art. 322 bis c.p.)

L'articolo in oggetto prevede che le ipotesi di reato sopra analizzate si applichino anche nei confronti dei seguenti soggetti, i quali sono assimilati ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi:

- Membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- Funzionari e agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- Persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- Membri e addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- Coloro che, nell'ambito di altri Stati membri dell'Unione europea svolgono funzioni e attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- Persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali.

Le pene previste sono le stesse degli artt. 314, 316,320,322 c.p.

13.7. Attività sensibili relative ai reati contro la Pubblica Amministrazione

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

essenzialmente:

- Attività nelle quali si instaura un rapporto contrattuale con la P.A. (si intende principalmente AdSP, beneficiaria dell'80 % circa del fatturato della Società per servizi e manutenzioni (*A titolo d'esempio si*

considerino i processi di aggiudicazione e gestione di commesse pubbliche, i contratti di finanziamento su progetti di rilievo pubblicistico, i rapporti con uffici del Ministero del Lavoro o Enti previdenziali);

ed anche:

- Attività relative alla gestione degli acquisti,

invece, in misura variamente secondaria e residuale:

- Attività relative alla gestione delle consulenze e delle liberalità;
- Nelle quali si instauri un rapporto con le istituzioni e/o le Autorità di Vigilanza;
- Che comportino la gestione delle verifiche e delle ispezioni;
- Che comportino la gestione dei servizi informatici.
- Che comportino la gestione dell'erogazione del credito anche attraverso fondi pubblici, sia nella fase d'acquisizione che dell'erogazione di contributi, in qualsiasi modo denominati, destinati a pubbliche finalità, sia nello svolgimento di funzioni in regime di concessione, in quanto regolate da norme di diritto pubblico ed atti autoritativi (*A titolo d'esempio, si considerino i processi di acquisizione e gestione di finanziamenti agevolati per interventi formativi, finanziamenti a Clientela con agevolazioni pubbliche, rapporti di Tesoreria con Enti della P.A., riscossione tributi, servizi di concessione, pagamento e custodia per conto della P.A. - pensioni, etc.);*

13.7. Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni nello svolgimento delle proprie attività commerciali, finanziarie, di informazione e di controllo sia in favore della società stessa sia in favore del Socio Unico e di altri possibili destinatari delle attività fornite da PTS.

- Ufficio protocollo - Coordinamento Acquisti

  L'attività presenta profili di rischio nella gestione degli acquisti della Società e per l'approvvigionamento dei beni e servizi a favore della stessa;

- Consiglio di Amministrazione

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

- Servizio Amministrazione.

  L'attività di questa funzione si considera a rischio per la gestione della corretta rappresentazione dei risultati economici della Società.

Ai fini della commissione dei reati contro la Pubblica Amministrazione è necessaria l'instaurazione di rapporti di natura contrattuale e non contrattuale con Pubblici Ufficiali e/o Incaricati di Pubblico Servizio appartenenti alla Pubblica Amministrazione, agli enti pubblici e/o ai soggetti ad essi assimilati facenti parte dello Stato italiano, delle Comunità Europee e degli Stati esteri. In tal senso, la sussistenza delle Convenzioni sopra cit. (Quadro, Manutenzioni e Servizi) non può essere di per sé assimilata ad un normale rapporto contrattuale, data la qualifica di PTS come *"longa manus"* di AdSP.

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

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

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

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

Le attività che la Società ha individuato come sensibili, nell'ambito dei reati contro la Pubblica Amministrazione, sono indicate nello specifico nella matrice delle attività a rischio reato, unitamente a possibili esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Di seguito vengono riepilogate le attività, di cui sopra:

- Gestione dei rapporti con i funzionari degli Enti pubblici finanziatori (Ministeri, Regione, Provincia, Istituti Comunitari, etc.), per ottenere l'erogazione di fondi pubblici finalizzati, a titolo esemplificativo, all'attuazione di piani formativi aziendali;
- Presentazione di istanze agli enti pubblici competenti in merito ad atti o provvedimenti amministrativi di interesse aziendale quali, a titolo esemplificativo, quelli relativi alla manutenzione degli immobili (ristrutturazione) e agli adempimenti in materia di sicurezza, salute, igiene sul lavoro e in ambito ambientale;
- Gestione dei rapporti con i funzionari degli Enti competenti in merito agli adempimenti societari presso la CCIAA, IL Tribunale e l'ufficio di registro;
- Gestione dei rapporti con i funzionari competenti (Inps, Inail, Asl, Direzione Provinciale del Lavoro, ecc.), anche in occasione di verifiche o ispezioni, per il rispetto degli obblighi previsti dalla normativa di riferimento;
- Gestione dei rapporti con le autorità di controllo (VVFF, ASL, Ispettorato del Lavoro, ecc.) in materia di tutela della salute e sicurezza sul lavoro, anche in sede di verifiche ispettive;
- Gestione dei rapporti con funzionari di Enti pubblici in merito all'assolvimento dell'obbligo di assunzione dei disabili;
- Predisposizione, sottoscrizione e invio della documentazione relativa ad una richiesta per ottenere l'erogazione di un finanziamento pubblico;
- Gestione dell'accesso al sistema informatico;
- Selezione e assunzione del personale;
- Gestione dei flussi monetari;
- Gestione del servizio acquisti (beni e servizi con soggetti privati);
- Gestione degli affidamenti;
- Gestione dei rapporti con i soggetti indagati o imputati in un procedimento penale nel quale la società sia co-imputata o si sia costituita parte civile;

- Gestione dei rapporti con i Giudici, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito di procedimenti giudiziari, civili, penali e amministrativi, che coinvolgono direttamente la Società;
- Gestione dei rapporti con soggetti terzi (ad es. fornitori) per la definizione di situazioni precontenziose o di contenziosi intrapresi da terzi nei confronti della Società o viceversa.

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

13.8. Principi e regole generali di comportamento

Si individuano qui di seguito i principi che informano le specifiche procedure interne della Società previste in relazione a qualsiasi operazione/attività che coinvolga un ente della Pubblica Amministrazione (che sia diverso dall'AdSP, in considerazione del rapporto di immedesimazione organica), nonché le regole di condotta che sottendono alle specifiche previsioni di comportamento elaborate dalla Società in relazione a tale ambito di applicazione.

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

Principi

Tutte le operazioni/attività che coinvolgono in qualsiasi modo un ente della Pubblica Amministrazione (diverso dall'AdSP) devono essere poste in essere nel pieno rispetto delle leggi vigenti, del Codice Etico delle regole contenute nel presente Modello, delle policy e delle procedure aziendali, dei valori e delle politiche della Società.

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

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

- Conoscibilità all'interno della Società;
- Chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri.

Il sistema di deleghe e procure.

In linea di principio il sistema di deleghe e procure, formalizzato nello Statuto e in documenti approvati dal Consiglio di Amministrazione e sopra richiamato (parte 11.4), stabilisce espressamente le facoltà di autonomia gestionale per natura di spesa e di impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione.

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

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

- Le funzioni che intrattengono per conto della Società rapporti con la P.A. devono essere individuate e preferibilmente dotate di delega formale in tal senso;
- Ciascuna delega deve definire in modo specifico I poteri del delegato;
- I poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- Il delegato deve disporre di eventuali poteri di spesa adeguati alle funzioni conferitegli.

L’Organismo di Vigilanza verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni 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.

Regole di comportamento.

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

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

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

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

- Promettere, offrire o acconsentire all’elargizione di denaro o altre utilità (beni materiali, servizi, etc.) a pubblici ufficiali o incaricati di pubblico servizio, o a loro familiari, che possano influenzare l’indipendenza del giudizio o indurre ad assicurare un vantaggio per la Società;
- Accordare vantaggi di qualsiasi natura (promessa di assunzione, etc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al punto precedente;
- Distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale) ed in particolare, è vietata qualsiasi forma di regalo a funzionari pubblici o a loro familiari, che possa influenzare l’indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l’azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o la brand image della società. I regali offerti - salvo quelli di modico valore, devono essere documentati in modo adeguato, per consentire le verifiche da parte dell’Organismo di Vigilanza;

- Mettere in atto o favorire operazioni in conflitto di interesse della Società, nonché attività in grado di interferire con la capacità di assumere decisioni imparziali nell'interesse della Società, nel rispetto del Codice Etico e delle normative applicabili;
- Ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque sia o intenda entrare in rapporto con la Società e voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite dalla Società o, comunque, un trattamento più favorevole di quello dovuto;
- Eseguire prestazioni o riconoscere compensi in favore dei collaboratori esterni e dei partner che non siano adeguatamente giustificati in ragione del rapporto contrattuale in essere con la Società;
- Effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati, o comunque utilità a carico di bilanci pubblici, e/o per partecipare a gare o simili o risultarne vincitori;
- Effettuare comunque dichiarazioni o attestazioni non veritiere ad organismi pubblici tali da indurre in errore tali soggetti, da creare un indebito profitto o vantaggio a favore della Società e/o arrecare un danno all'ente pubblico;
- Destinare eventuali somme ricevute da enti pubblici nazionali e/o comunitari per scopi diversi da quelli a cui originariamente erano destinati.

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

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

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

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

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

- Formale identificazione del soggetto deputato ad intrattenere rapporti con la Pubblica Amministrazione in relazione a ciascuna Potenziale Attività a Rischio;
- Gestione in modo trasparente e univoco di qualsiasi rapporto professionale instaurato con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- Attività di reporting all'Organismo di Vigilanza di eventuali situazioni di irregolarità.

13.9. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

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

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

- Agli Organi Sociali, Dipendenti, Consulenti e Partner che materialmente intrattengono rapporti con la Pubblica Amministrazione per conto della Società deve essere formalmente conferito potere in tal senso (con apposita delega per i membri degli organi sociali e per i dipendenti - anche tramite il responsabile, individuato in base al sistema delle comunicazioni organizzative, ovvero nel relativo contratto di servizio o di consulenza o di partnership per gli altri soggetti destinatari del Modello);
- I contratti tra la Società, i Consulenti e Partner che abbiano, anche solo potenzialmente, impatto sulle Potenziali Aree a Rischio devono essere definiti per scritto in tutte le loro condizioni e termini e devono contenere clausole standard al fine di garantire il rispetto del D. L.gs. 231/2001;
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi, finanziamenti, ed in genere di benefici a carico di bilanci pubblici, devono contenere solo elementi veritieri e l'impegno della Società, in caso di ottenimento degli stessi, all'effettiva utilizzazione dei fondi ottenuti secondo le finalità previste dalla specifica normativa di riferimento. In ogni caso, ciascuna delle dichiarazioni di cui al presente capo, ivi incluse le autocertificazioni ammesse dalla legge o dai bandi, devono essere corredate da documentazione idonea ad attestarne la veridicità, anche se eventualmente non richiesta dal destinatario di tali dichiarazioni;
- Alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D. L.gs. 81/08 e successive modifiche, a verifiche tributarie, INPS, etc.) devono possibilmente partecipare i soggetti a ciò espressamente delegati, dando avviso dell'avvio dell'ispezione/accertamento al Consiglio di Amministrazione, al Presidente del Consiglio di Amministrazione e al Direttore Generale oltre che all'Organismo di Vigilanza. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati appositi verbali. Nel caso il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta;
- La stipulazione di contratti/convenzioni con soggetti pubblici (diversi da AdSP) da parte della Società a seguito della partecipazione a procedure ad evidenza pubblica (asta pubblica, appalto-concorso, licitazione privata e trattative private) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello;
- Ai Collaboratori esterni e Partner che materialmente intrattengono rapporti con la Pubblica Amministrazione (inclusa AdSP) per conto della Società, deve essere formalmente conferito potere in tal senso dalla Società stessa;
- Ci deve essere una tendenziale separazione dei compiti tra chi effettua l'ordine di acquisto o sottoscrive un contratto e chi registra ed autorizza il pagamento della rispettiva fattura;
- L'Organismo di Vigilanza deve essere informato con nota scritta di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la Pubblica Amministrazione;
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di concessioni, autorizzazioni o licenze devono esser per iscritto e contenere solo elementi assolutamente veritieri.

- Gli affidamenti sotto soglia vengono effettuati nel rispetto del Regolamento acquisti adottato da PTS e approvato da AdSP nel rispetto del Dlgs 50 /2016 e delle vigenti linee Guida ANAC.

13.10. I controlli dell'Organismo di Vigilanza

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

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

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

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

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

PARTE QUATTORDICESIMA

REATI SOCIETARI

14.1. Le fattispecie di reato richiamate dal D. L.gs 231/2001

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

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

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

a. False comunicazioni sociali (Artt. 2621, 2621 bis, 2621 ter c.c.)

Questo reato si realizza tramite:

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

La pena prevista per tale reato dall'art. 9. della legge n.69 del 27 maggio 2015 che ha modificato l'art. 2621, è la reclusione da uno a cinque anni

L'art. 10. della legge n. 69 del 27 maggio 2015 introduce gli articoli 2621 bis e ter del codice civile e recitano:

> **Art. 2621-bis Fatti di lieve entità**
>
> *Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.*
>
> **Art. 2621-ter Non punibilità per particolare tenuità**
>
> *Ai fini della non punibilità per particolare tenuità del fatto, di cui all'articolo 131-bis del codice penale, il giudice valuta, in modo prevalente, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori conseguente ai fatti di cui agli artt.2621 e 2621bis.*

Si precisa che:

- La condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- Le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;

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

Esempio

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

b. *Impedito controllo (Art. 2625 c.c.)*

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

Il reato è punito con la sanzione amministrativa di 10.329 euro.

Se la condotta ha però cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Esempio

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

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

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

La pena prevista è fino ad un anno di reclusione.

d. *Illegale ripartizione degli utili o delle riserve (Art. 2627 c.c.)*

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva; ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

La pena prevista è fino ad un anno di reclusione.

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.

Esempio

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

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

Questo reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Questo reato non sembra potersi realizzare neppure in astratto, in quanto la controllante non è una società commerciale ma un ente pubblico non economico.

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

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

Il reato è punito, a querela della persona offesa, da sei mesi a tre anni.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Esempio

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

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

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

Esempio

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

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

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

Il reato è punito, a querela della persona offesa, da sei mesi a tre anni.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

i. *Corruzione tra privati (Art. 2635 c.c.)*

L'art.3 del D. L.gs n. 38 del 15 marzo 2017 recita: «Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni.

Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.

Le pene stabilite sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

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

La misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse o offerte.

j. Istigazione alla corruzione tra privati (Artt. 2635 bis, 2635 ter c.c.)

Il D. L.gs n. 38 del 15 marzo 2017 con l'art.4 ha introdotto il suddetto reato che recita:

"*Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.*

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

Si procede a querela della persona offesa."

Dopo l'articolo 2635-bis l'art.5 del D. L.gs 38 ha inserito l'art. 2635-ter che recita:

"La condanna per il reato di cui all'articolo 2635, primo comma, importa in ogni caso l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'articolo 32-bis del codice penale nei confronti di chi sia già stato condannato per il medesimo reato o per quello di cui all'articolo 2635-bis, secondo comma.".

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

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

La pena prevista è da sei mesi a tre anni di reclusione

Esempio

Il Consiglio di Amministrazione della società, al fine di ottenere una deliberazione favorevole del socio unico, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso Consiglio di Amministrazione intende acquisire, in modo da ricavarne un indiretto profitto.

l. Aggiotaggio (Art. 2637 c.c.)

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

La pena prevista è da uno a cinque anni di reclusione.

Esempio

Il Direttore Generale dell'azienda diffonde al mercato la notizia del mancato rilascio da parte societaria di una polizza fideiussoria richiesta nell'ambito di un'operazione avente ad oggetto il trasferimento di azioni di una società non quotata. A causa di tale comunicazione il potenziale acquirente rinuncia a concludere il contratto di compravendita dei suddetti titoli.

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

Poiché la Società,—non risulta soggetta direttamente alla vigilanza di autorità pubbliche (a differenza ad es. dell'Autorità di Sistema Portuale), non si ritiene rilevante tale reato.

14.2. Le attività sensibili relative ai reati societari

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

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

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

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

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

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

Principali Aree a rischio e attività sensibili interessate:

Gestione della Contabilità:

- Imputazione delle scritture contabili in contabilità generale;
- Verifiche sui dati contabili immessi a sistema e quelli inviati al consulente esterno;
- Predisposizione di bilanci e documentazione di natura contabile: si tratta delle attività relative alle chiusure contabili, alla contabilizzazione dei dati e alla predisposizione del bilancio d'esercizio della Società e dei relativi allegati;

Segreteria Generale - Direzione

- Predisposizione di documenti ai fini delle delibere assembleari e delle decisioni del Consiglio di Amministrazione: si tratta delle attività di predisposizione della documentazione relativa all'oggetto dell'Assemblea e del Consiglio di Amministrazione per consentire a quest'ultimo di esprimersi sulle materie di propria competenza sottoposte ad approvazione;
- Gestione delle comunicazioni verso soci: si tratta dell'attività di predisposizione della documentazione oggetto di comunicazioni verso soci.

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

a) degli standard di controllo generali;

b) dei principi di comportamento individuati nel Codice Etico;

c) di quanto regolamentato dalla documentazione e dagli atti aziendali;

d) delle disposizioni di legge.

14.3. Organi e funzioni aziendali coinvolte

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

Consiglio di Amministrazione.

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

Presidente del C.d.A.

I profili di rischio attengono alle funzioni attribuitegli dalla legge;

Aree: Amministrazione.

L'attività di questa funzione si considera a rischio per la gestione della corretta rappresentazione dei risultati economici, degli adempimenti fiscali e le comunicazioni al Collegio sindacale ed ai soci.

Uffici Relazioni esterne e Affari legali societari.

L'attività presenta profili di rischio nella gestione delle comunicazioni istituzionali e le relazioni con le istituzioni.

Responsabile anticorruzione e trasparenza.

A riguardo delle attività a rischio reato di corruzione tra privati e di istigazione alla corruzione tra privati, l'RPCT si coordinerà costantemente con l'OdV.

14.4. Principi e regole generali di comportamento

Per quanto concerne le fattispecie criminose che si riferiscono ai documenti contabili ed ai controlli del Collegio sindacale, si rileva che la Società si pone in una posizione privilegiata dal punto di vista della prevenzione e della corretta attuazione dei precetti normativi, in quanto risulta destinataria di una disciplina speciale che impone la procedimentalizzazione dell'intera fase di elaborazione di detta documentazione, nonché una serie di obblighi ed adempimenti in relazione ai rapporti con il Sindaco ed il Socio Unico.

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

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

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

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

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

- La normativa italiana e straniera applicabile alle attività svolte;
- Il Codice Etico e di comportamento;
- Il presente Modello 231;
- Le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della Società.

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

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

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

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

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

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

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

14.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

É evidente che contribuiscono a mitigare il rischio di commissione dei alcuni op tutti i reati societari in parola, le seguenti circostanze:

- La tipologia di s.r.l. rende inapplicabili le norme incriminatrici riferite specificamente alle azioni ed alle obbligazioni;
- La partecipazione totalitaria di AdSP risulta incedibile per legge, anche in parte;
- Il "mercato" (concetto più volte richiamato nel presente ambito penal-societario) per PTS non è costituito dalla collettività potenziale ed indifferenziata degli operatori economici, ma per ben l'80 % dall'ente pubblico non economico APT;
- Il "controllo analogo" vincola, anche sotto forma di controlli preventivi e vere e proprie autorizzazioni, l'operatività di PTS, specie a livello di straordinaria amministrazione e in caso di operazioni straordinarie.

Gli Amministratori, il Sindaco, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto di PTS, dovranno tener conto, oltre a quanto precedentemente descritto e relativamente ad ognuna delle fattispecie di reato ritenute rilevanti per la Società, delle previsioni di seguito indicate.

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

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

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

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

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

b) Omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;

c) Porre la massima attenzione e accuratezza nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni utilizzati in modo tale da fornire una presentazione veritiera e corretta corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività.

d) Provvedere o far provvedere tempestivamente alla comunicazione delle situazioni semestrali al socio unico nonché a tutte le altre comunicazioni periodiche previste dallo Statuto.

Inoltre, gli Organi Sociali, gli Amministratori, i dipendenti nonché i collaboratori della Società e della controllata dovranno tener conto, oltre a quanto precedentemente definito delle procedure e regole aziendali che prevedono:

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

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

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

a. Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;

b. Tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative agli strumenti finanziari emessi da altre Società del Gruppo, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società, sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti;

c. 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;

d. Assicurare il regolare funzionamento degli Organi Societari, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

e. Evitare di porre in essere operazioni simulate o diffondere notizie false idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari;

f. Effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

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

- Con riferimento al precedente punto 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
  - Omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società.
- Con riferimento al precedente punto b:
  - Alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi eventualmente predisposti dalla Società;
  - Illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti.
- Con riferimento al precedente punto c:
  - Restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
  - Ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
  - Acquistare o sottoscrivere azioni o quote della società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
  - Effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;

- Procedere a formazione e/o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale.

- Con riferimento al precedente punto d:
  - Porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione della gestione sociale da parte del collegio sindacale o della società di revisione o che comunque la ostacolino;
  - Determinare o influenzare l'assunzione delle deliberazioni dell'Assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.
- Con riferimento al precedente punto e:
  - Pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio aventi ad oggetto strumenti finanziari non quotati e idonei ad alterarne sensibilmente il prezzo ovvero al fine di incidere sul pubblico affidamento in merito alla stabilità patrimoniale societaria.
- Con riferimento al precedente punto f:
  - Omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle autorità di vigilanza cui è soggetta l'attività aziendale, nonché omettere di dar corso con sollecitudine all'invio dei dati e della documentazione eventualmente richiesta dalle predette autorità;
  - Esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
  - Porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità.

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

Predisposizione delle comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Società.

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

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

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

- Verificabilità, documentabilità, tracciabilità, coerenza e congruenza di ogni operazione;
- Documentazione delle decisioni e dei controlli;
- Accurata gestione delle notizie riservate.

Predisposizione dei prospetti informativi.

La redazione, o partecipazione alla redazione, di prospetti informativi dovrà essere effettuata sulla base di procedure che si fondano sui seguenti principi:

- Utilizzo di procedure coerenti con quelle adottate per la predisposizione delle comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Società;
- Ove esistenti, utilizzo di informazioni contenute in comunicazioni già pubblicate;
- Utilizzo di informazioni previsionali condivise dalle funzioni coinvolte ed approvate dal Consiglio di Amministrazione.

Operazioni relative al capitale sociale

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

Altre regole finalizzate alla prevenzione dei reati societari in genere

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

- Previsione di riunioni tra Sindaco e Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di *corporate governance*;
- Trasmissione al Sindaco, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge;
- Partecipazione dell'Organismo di Vigilanza alle riunioni assembleari mediante apposito invito. L'Organismo di Vigilanza valuterà l'utilità della propria partecipazione.

14.6. I controlli dell'Organismo di Vigilanza

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

L'Organismo di Vigilanza dovrà avere evidenza e mantenere traccia di quanto posto in essere nella Società al fine di fornire opportune indicazioni per la corretta redazione del bilancio.

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

L’Organismo di Vigilanza si coordinerà costantemente con la Responsabile Anticorruzione e Trasparenza a riguardo delle attività a rischio reato in materia bilancistica e societaria.

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

- Proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- Monitorare sul rispetto delle procedure interne per la prevenzione dei reati societari.
- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

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

PARTE QUINDICESIMA

REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI

15.1. Le fattispecie di reato richiamate dal D. L.gs. 231/2001

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

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

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

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

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

a. Falsità in documenti informatici (Art. 491 bis c.p.)

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

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

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

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

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

A tal proposito il D. L.gs 7 del 15 gennaio 2016 aggiunge: "*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici".*

b. *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". Tale delitto è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

- 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;
- Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- Se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora 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, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

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.

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

Tale reato si realizza quando un soggetto, "*al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo*".

Tale reato è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se il danno è commesso:

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

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

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

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

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

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

d. Diffusione 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici".

Tale reato è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

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 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

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

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.

Tale reato è punito con la reclusione da sei mesi a quattro anni.

La pena è della reclusione da uno a cinque anni:

- 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;
- Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 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 fraudolenza 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 si integra, 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.

f. Installazione di apparecchiature atte 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, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi*". Tale reato è punito con la reclusione da uno a quattro anni.

La condotta vietata dall'art. 617-quinquies è, pertanto, costituita dalla mera installazione delle apparecchiature, 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 installazione di apparecchiature idonee 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 abbia, obiettivamente, una potenzialità lesiva.

Qualora all'installazione 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.

g. *Danneggiamento di informazioni, dati e programmi informatici (Art. 635 c.p.)*

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

Tale reato è punito con la reclusione da sei mesi a tre anni.

Il D. L.gs 7 del 15 gennaio 2016 recita: "*Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità' di operatore del sistema, la pena è della reclusione da uno a quattro anni.".*

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.

h. *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*".

Tale reato è punito con la reclusione da uno a quattro anni.

La sanzione è da tre a otto anni se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

Il D. L.gs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è 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.

i. 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*".

Tale reato è punito con la reclusione da uno a cinque anni.

Il D. L.gs 7 del 15 gennaio 2016 recita: "*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 si integra 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).

j. 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*". Tale reato è punito con la pena della reclusione da uno a quattro anni.

La sanzione è della reclusione da tre a otto anni 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.

Il D. L.gs 7 del 15 gennaio 2016 recita: "*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.

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

Questo reato si configura quando chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

La pena prevista è la reclusione da sei mesi a tre anni e la multa da € 51 a € 1.032.

La pena va da uno a cinque anni e la multa da € 309 a € 1.549 se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Se poi il fatto è commesso con furto e indebito utilizzo in danno di qualcuno la reclusione va da due a sei anni e la multa da € 600 a € 3.000.

Il delitto è punibile a querela della persona offesa, salvo che ricorra un'altra circostanza aggravante.

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

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

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

15.2. Le attività sensibili relative ai reati informatici

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

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

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

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

- Tutte le attività aziendali svolte dal personale tramite l'utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad Internet
- Gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica
- Erogazione di servizi di installazione e servizi professionali di supporto al personale (ad esempio, assistenza, manutenzione, gestione della rete, manutenzione e security)

Occorre considerare in proposito che la clientela-tipo della Società non è della categoria "retail" ma corporate, ed essenzialmente è il Socio Unico e per il 20 % al massimo da soggetti strutturati (quali compagnie

ed agenti marittimi, spedizionieri e trasportatori) che hanno proprie barriere di accesso, rendendo per ciò remoto il rischio di commissione dei reati informatici qui commentati.

Deve, sul punto segnalarsi che, gli accessi da parte degli utenti alle aree portuali, pur custodite da PTS, sono trattati e registrati a cura di AdSP, a cui fa capo quindi la nomina del DPO.

Il personale PTS ai varchi procede infatti all'identificazione dell'utente ma non alla conservazione dei dati così ottenuti (attività di competenza AdSP).

Risulterà opportuno effettuare un approfondimento delle conclusioni raggiunte in materia di trattamento dati, di reati informatici e di normativa privacy allorquando, e nel caso in cui, AdSP procederà al trasferimento in capo a PTS del progetto "Porto Digitale".

15.3. Organi e funzioni aziendali coinvolte

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

- Consiglio di Amministrazione

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

- Responsabili acquisti e Ufficio Sistemi Informativi

Tale funzione viene considerata coinvolta nelle Attività Sensibili, avendo come compito quello di tenere le relazioni con i potenziali clienti.

- Responsabile trattamento dati e Privacy

Tale funzione viene considerata coinvolta nelle Attività Sensibili, avendo come compito quello di applicare ed aggiornare la recente disciplina "Privacy" basata sul regolamento UE 679/2016, in vigore dal 25 maggio 2018, adeguando opportunamente la *compliance* aziendale.

15.4. Principi e regole generali di comportamento

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

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

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Società, ivi inclusa la controllata, devono conoscere e rispettare:

1. Gli standard generali di controllo;
2. I principi di comportamento individuati nel Codice Etico;
3. Quanto regolamentato dalla documentazione e dagli atti aziendali;
4. Le disposizioni di legge.

Fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale ed al fine di perseguire la prevenzione dei Reati Informatici è fatto espresso divieto a tutti i Soggetti coinvolti di

porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 24-bis del D. L.gs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale.

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

- Previsione nel Codice Etico di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno della società che tramite apparecchiature non soggette al controllo della stessa;
- Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite;
- Predisposizione di adeguati strumenti tecnologici atti a prevenire e/o impedire la realizzazione di reati informatici da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio;
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.

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

- Esistenza di procedure
  Devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività;
- Poteri autorizzativi e di firma
- Definire livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio;
- Tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio; ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione distruzione delle registrazioni effettuate;
- Gestione delle segnalazioni

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

- Riporto all'Organismo di Vigilanza
  Riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

15.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

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

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

- Esistenza di una normativa/procedura aziendale relativa a:
  1. Gestione degli accessi che tra l'altro individua le seguenti fasi:
     - Attribuzione accessi;
     - Assegnazione dei codici identificativi personali (richieste di abilitazione/modifica delle utenze);
     - Disattivazione dei codici utente associati al personale che ha perso il diritto di accesso a tutti i sistemi informatici o che non accede più ai vari sistemi;
     - Attività di controllo volta a verificare, prima della creazione di un'utenza, che la stessa non sia già stata precedentemente assegnata/disabilitata/rimossa e che uno stesso codice identificativo personale non venga assegnato, neppure in tempi diversi, a persone diverse.
  2. Modalità di utilizzo e di salvaguardia del PC intese come misure che l'utente deve adottare per garantire un'adeguata Protezione delle apparecchiature incustodite;
  3. Installazione di software sui sistemi operativi;
  4. Dismissione dei supporti di memorizzazione su cui sono registrate informazioni aziendali.
- Presenza di sistemi di protezione antivirus e antispam;
- Esistenza di una serie di procedure, in materia di *"privacy"* e di *"security"*, che disciplinano gli aspetti legati al corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- Attuazione del progetto di formazione, volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy;
- Attuazione di programmi di formazione specifica per tutti gli addetti ai varchi, al portierato, al portierato/*security*.
- Consegna a ciascun dipendente della Società, contestualmente all'assegnazione del pc e/o dell'indirizzo di posta internet di norme per l'utilizzo dei Personal Computer aziendali e sull'utilizzo della posta internet e in generale di documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico;
- Individuazione tempestiva delle vulnerabilità dei sistemi;
- Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse

tecnologiche e informazioni), attraverso, l'adozione di sistemi antincendio, antiallagamento, di condizionamento, gruppi di continuità UPS e di regolamentazione degli accessi;

- Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici (registrazione dei *log on e log off*).

Si elencano, qui di seguito, le regole che devono essere rispettate dalla Società e dai dipendenti e dagli altri soggetti eventualmente autorizzati nell'ambito delle Attività Sensibili.

- I dati e le informazioni non pubbliche, relative ad AdSP e agli altri clienti, potenziali clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati;
- È vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili;
- È vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- È vietato divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;
- È obbligatorio segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

PTS si impegna a porre in essere i seguenti adempimenti:

- Informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi (cfr. Manuale utilizzo User ID e password);
- Fare sottoscrivere ai dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali;
- Informare i dipendenti e agli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso (cfr. Manuale utilizzo User ID e password);
- 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;
- Fornire ogni sistema informatico di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- Impedire l'installazione e l'utilizzo di software non approvati dalla società e non correlati con l'attività espletata per la stessa;

- Limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file);
- Qualora per la connessione alla rete Internet si utilizzino collegamenti *wireless* (ossia senza fili, mediante *routers* dotati di antenna WiFi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;
- Prevedere un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati;
- Limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti e degli altri soggetti eventualmente autorizzati (i.e. connessione tramite VPN o RAS);
- Effettuare periodicamente, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile, controlli *ex ante* ed *ex post* sulle attività effettuate dal personale sulle reti nonché rielaborare con regolare cadenza i log dei dati al fine di evidenziare eventuali comportamenti anomali.

15.6. I controlli dell'Organismo di Vigilanza

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

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

- Svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24-bis del Decreto; con riferimento a tale punto, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di delitti informatici, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti informatici di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche;
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale;
- Monitorare il rispetto delle procedure e la documentazione interna (i.e. Normativa Aziendale e Modulistica) per la prevenzione dei Delitti Informatici;

- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- Conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

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

PARTE SEDICESIMA

REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI O UTILITÁ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO

16.1. Le fattispecie di reato richiamate dal D. L.gs. 231/2001

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

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

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

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

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

La presente Parte Speciale si riferisce ai reati di riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'art. 25-*octies* del D. L.gs. n. 231/01 prevede una responsabilità dell'ente nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio dell'ente stesso.

a. 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 comunque si intromette nel farli acquistare, ricevere od occultare.

Tale ipotesi è punita con la reclusione da due a otto anni e con la multa da euro 516 ad euro 10.329. La pena è diminuita quando il fatto è di particolare tenuità.

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

La pena è aumentata secondo il DL n.93 del 14 agosto 2013, modificato dalla L. n.119 del 15 ottobre 2013 quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata, di estorsione aggravata o di furto aggravato.

b. *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 non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

La pena per tale reato, prevista dall'art. 3 della L. n.186 del 15 dicembre 2014, è la reclusione da quattro a dodici anni e la multa da euro 5.000 a euro 25.000.

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

c. *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.

La pena per tale reato, prevista dall'art. 3 della L. n. 186 del 15 dicembre 2014, è la reclusione da quattro a dodici anni e la multa da euro 5.000 a euro 25.000.

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

La normativa italiana in tema di prevenzione dei Reati di Riciclaggio prevede norme tese ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione e l'adeguata verifica della clientela e la registrazione dei dati in appositi archivi.

Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal Decreto Antiriciclaggio, che in parte ha abrogato e sostituito la Legge 197/1991

Il Decreto Antiriciclaggio prevede in sostanza i seguenti strumenti di contrasto del fenomeno del riciclaggio di proventi illeciti:

1. La previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore a euro 5.000. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.a.;
2. L'obbligo di adeguata verifica della clientela da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) in relazione ai rapporti ed alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi. In tale ambito rientra anche l'obbligo della clientela di fornire, sotto la propria responsabilità, tutte le informazioni necessarie ed aggiornate per consentire agli intermediari di adempiere agli obblighi di adeguata verifica;
3. L'obbligo di astenersi dall'apertura del Rapporto Continuativo o dall'esecuzione dell'operazione qualora l'intermediario non sia in grado di rispettare gli obblighi di adeguata verifica della clientela;
4. L'obbligo da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;
5. L'obbligo di segnalazione da parte di alcuni soggetti (elencati agli artt. 10, comma 2, 11, 12, 13 e 14 del Decreto Antiriciclaggio) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al territorio.

I soggetti sottoposti agli obblighi di cui ai nn. 2., 3., 4. sono, tra gli altri:

- Gli intermediari finanziari e gli altri soggetti esercenti attività finanziaria. Tra tali soggetti figurano:
- Banche;
- Poste italiane;
- Società di intermediazione mobiliare;
- Società di gestione del risparmio;
- Società di investimento a capitale variabile;
- Le imprese di assicurazione che operano in Italia nei rami di cui all'art. 2, comma 1, del CAP (rami vita);
- I professionisti, tra i quali si indicano:
- I soggetti iscritti nell'albo dei ragionieri e periti commerciali;
- I notai e gli avvocati quando, in nome e per conto dei loro clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i loro clienti in determinate operazioni;
- I revisori legali;
- Altri soggetti, intesi quali operatori che svolgono alcune attività il cui esercizio resta subordinato al possesso delle licenze, autorizzazioni, iscrizioni in albi o registri, ovvero alla preventiva dichiarazione di inizio di attività richieste dalle norme;

Tra le attività si indicano:

- Recupero di crediti per conto terzi;
- Trasporto di denaro contante;
- Gestione di case da gioco;
- Offerta, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro.

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

La legge n. 186 del 15 dicembre 2014 ha inserito il reato di autoriciclaggio che si commette quando si impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di un delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

La pena prevista è la reclusione da due a otto anni e la multa da euro 5000 a euro 25000

La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale, invece è diminuita fino alla metà per chi 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.

16.2. Le attività sensibili relative ai reati di ricettazione, riciclaggio ed impiego di denaro, bene o utilità di provenienza illecita, nonché autoriciclaggio

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

- Accensione di rapporti continuativi, quali ad esempio:
  - Conti correnti;

- Deposito titoli;
- Depositi a risparmio.

- Esecuzione di operazioni disposte dalla Clientela, quali ad esempio:
  - Operazioni di versamento contante;
  - Operazioni su assegni bancari o circolari;
  - Operazioni su strumenti finanziari;
  - Rapporti con i fornitori.

16.3. Organi e funzioni aziendali coinvolte

In relazione alle descritte attività sensibili tutte astrattamente ipotizzabili si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali.

Servizio Finanza (l'attività presente profili di rischio nella gestione degli acquisti aziendali e per l'approvvigionamento dei beni e servizi a favore di esso);

Consiglio di Amministrazione;

16.4. Principi e regole generali di comportamento

Obiettivo della presente Parte Speciale è che tutti i Destinatari, nella misura in cui gli stessi possano essere coinvolti nelle attività sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei reati di riciclaggio e autoriciclaggio.

Nell'espletamento delle attività aziendale e in particolare nelle aree sensibili, è espressamente vietato ai Destinatari di porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (art. 25-octies del Decreto).

In particolare, i Destinatari hanno l'obbligo di segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

16.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Ai fini dell'attuazione delle regole e dei divieti elencati precedentemente devono rispettarsi i principi procedurali qui di seguito descritti

In particolare, si elencano qui di seguito le regole che devono essere rispettate dalla Società e dai Destinatari nell'ambito delle attività sensibili, nonché più in generale nell'esercizio della sua attività

La società verifica l'attendibilità commerciale e professionale dei fornitori attraverso:

- Visure ordinarie presso la Camera di Commercio o certificati equivalenti per fornitori stranieri
- Analisi del fornitore per verificarne la coerenza con le prestazioni richieste

- Dichiarazione da parte del fornitore di non avere procedimenti penali a carico, con specifico riferimento alle norme penali e alle responsabilità in tema di falso

La società inserisce nei contratti con i fornitori una specifica clausola con la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali aziendali e dei principi contenuti nel Modello e si impegnino al rispetto degli stessi.

Il mancato rispetto dei comportamenti etici o false dichiarazioni relative alla situazione del fornitore di cui al paragrafo precedente comporteranno l'applicazione di una penale o, a seconda della gravità, la risoluzione del contratto.

PTS è in procinto di inserire, nei contratti con i collaboratori esterni e con i partner, un'apposita dichiarazione dei medesimi con cui afferma:

- Di essere a conoscenza della normativa di cui al Decreto 231, nonché dell'adozione da parte della stessa del Modello e del Codice etico;
- Di impegnarsi al rispetto delle prescrizioni contenute nel Decreto, nonché dei principi contenuti nel Modello e nel Codice Etico.

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

PTS prevede appositi corsi di formazione che abbiano ad oggetto i contenuti della normativa e delle procedure adottati dalla Società stessa in materia di contrasto al riciclaggio, nonché le modalità con cui deve agire un dipendente che si trovi a gestire un'operazione sospetta; la frequenza a tali corsi è obbligatoria e l'inosservanza è sanzionata disciplinarmente.

16.6. I controlli dell'Organismo di Vigilanza

Fermo restando il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di riciclaggio, commessi nell'interesse o a vantaggio della Società, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello

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

L'Organismo di Vigilanza dovrà, inoltre, esaminare eventuali segnalazioni specifiche provenienti dagli organi sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute

In particolare, per quanto concerne i reati di cui all'art. 25-octies, deve:

- Comunicare, senza ritardo, alle Autorità di vigilanza di settore tutti gli atti o i fatti di cui viene a conoscenza nell'esercizio dei propri compiti, che possano costituire una violazione delle disposizioni emanate ai sensi dell'art. 7, comma 2, del Decreto Antiriciclaggio;
- Comunicare, senza ritardo, al Consiglio di Amministrazione le infrazioni alle disposizioni di cui all'art. 41 del Decreto Antiriciclaggio di cui ha notizia;

- Comunicare, entro trenta giorni, al Ministero dell'economia e delle finanze le infrazioni alle disposizioni di cui all'art. 49, commi 1, 5, 6, 7, 12, 13 e 14 e all'art. 50 del Decreto Antiriciclaggio di cui ha notizia;
- Comunicare, entro trenta giorni, alla UIF le infrazioni alle disposizioni contenute nell'art. 36 del Decreto Antiriciclaggio di cui ha notizia.

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

PARTE DICIASETTESIMA

REATI AMBIENTALI

17.1. Le fattispecie di reato richiamate dal D. L.gs. 231/2001

Violazione del divieto di scarico sul suolo, nel suolo e nelle acque sotterranee, Art. 137, co.11, D.lgs. 152/2006

Ai sensi del predetto articolo, è sanzionata la condotta di chiunque, nel caso di scarico al suolo, non osservi i divieti di scarico previsti dagli Artt.103 e 104 del D.lgs.152/2006.

Omessa bonifica dei siti, Art. 257, D.lgs. 152/2006

Ai sensi del predetto articolo, è punito chiunque cagioni l'inquinamento del suolo, sottosuolo, delle acque superficiali o sotterranee, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti del D.lgs.152/2006.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei fornitori, Art.258 co. IV, D.lgs. 152/2006

Secondo quanto disposto dal suddetto articolo al comma IV, è punito chiunque predisponga un certificato di analisi dei rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, nonché il soggetto che utilizza un certificato falso durante il trasporto.

Attività organizzate per il traffico illecito dei rifiuti, Art. 260, D.lgs. 152/2006

L'Art. 260 del D.lgs. 152/2006 punisce chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti.

Sistema informatico di controllo della tracciabilità dei rifiuti (SISTRI), Art. 260 bis, D.lgs. 152/2006

Secondo quanto disposto dal suddetto articolo, è punito il soggetto che fornisce, nell'ambito del sistema di controllo e tracciabilità dei rifiuti, certificati di analisi di rifiuti contenenti informazioni incomplete o inesatte, ovvero altera fraudolentemente uno qualunque dei dispositivi tecnologici accessori al predetto sistema informatico di controllo, o comunque ne impedisce in qualsiasi modo il corretto funzionamento.
Tale fattispecie di reato riguarda tutte le imprese, gli enti produttori e trasportatori di rifiuti che aderiscono al SISTRI.

Reati in materia di ozono e atmosfera, Art.3, co. VI, L.549/1993

Ai sensi del predetto articolo è punito chiunque violi le disposizioni che impongono la cessazione dell'utilizzo di sostanze lesive dell'ozono, di cui alle tab. A e B della L. 549/2006, al fine di ottenere un illecito risparmio.

Inquinamento ambientale, Art.452 bis c.p.

Secondo quanto disposto dal predetto articolo, è punito chiunque abusivamente cagioni una compromissione o un deterioramento significativo e misurabile delle acque o dell'aria, o di porzioni estese o significative del suolo e del sottosuolo; di un ecosistema, della biodiversità anche agraria, della flora o della

fauna.
È inoltre previsto un incremento della pena per chiunque causi l'inquinamento in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette.

Disastro ambientale, Art.452 quater, c.p.

Il reato di cui all'Art. 452 quater c.p., si configura qualora un soggetto cagioni abusivamente un disastro ambientale mediante alterazione irreversibile dell'equilibrio di un ecosistema, o la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali; oppure l'offesa alla pubblica incolumità in ragione della rilevanza del fatto o dei suoi effetti lesivi per il numero delle persone offese o esposte al pericolo.
Come per il reato precedente, è previsto un aumento della pena, qualora il disastro sia prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette.

Delitti colposi contro l'ambiente, Art.452 quinquies, c.p.

Qualora i reati, di cui agli Artt. 452-bis e 452-quater c.p., siano commessi per colpa, le pene previste dai medesimi articoli sono diminuite da un terzo a due terzi. Nel caso in cui dalle condotte colpose derivi il pericolo di inquinamento ambientale o di disastro ambientale le pene, la norma dispone un ulteriore diminuzione delle pene pari ad un terzo.

17.2. Le attività sensibili relative ai reati ambientali

Le attività che la Società ha individuato come sensibili, nell'ambito dei reati ambientali sono indicate nello specifico nella matrice delle attività a rischio reato, unitamente a possibili esemplificazioni di modalità e finalità di realizzazione della condotta illecita.
Di seguito vengono riepilogate le attività, di cui sopra:

- Gestione dell'attività di raccolta, trasporto, recupero e smaltimento dei rifiuti generati nei siti aziendali, affidati a società terze;
- Gestione delle comunicazioni e degli adempimenti verso gli Enti pubblici relativi alla gestione del trasporto dei rifiuti;
- Gestione delle autorizzazioni e delle manutenzioni relative alla rete idrica;
- Gestione e controllo, da parte dei referenti di ogni area (servizi, manutenzione, etc.), della produzione di rifiuti pericolosi e non.
- Verifica delle condizioni delle rete fognaria ed eventuali segnalazioni a AdSP.

17.3. Organi e funzioni aziendali coinvolte

Per quanto riguarda le aree sensibili riferibili ai reati ambientali, si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali come:

- Consiglieri di Amministrazione;
- Direzione;
- Area manutenzioni;
- Area Servizi;

- Ufficio coordinamento acquisti.

17.4. Principi e regole generali di comportamento

PTS, nel rispetto del Codice Etico e di Comportamento adottato ed in particolare del punto 6 dei "Codici di condotta" del citato documento, si impegna a perseguire la tutela dell'ambiente, avendo come obiettivo il miglioramento continuo delle proprie prestazioni ambientali. Per tale ragione, tutti i Destinatari del Modello, nello svolgimento delle attività sensibili sopra citate, sono tenuti ad osservare i seguenti principi di comportamento e controllo.

In generale a tutti i Destinatari è richiesto di:

- Rispettare la normativa ambientale vigente;
- Non effettuare attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione;
- Non cagionare l'inquinamento del suolo, sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio e, nel caso, provvedere alla bonifica;
- Nella predisposizione di un certificato di analisi di rifiuti, fornire le corrette indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti medesimi;
- Non effettuare il traffico illecito di rifiuti;
- Non superare i valori limite di emissione di qualità dell'aria previsti da eventuali autorizzazioni, prescrizioni e dalla normativa vigente;
- Non effettuare scarichi di acque reflue senza autorizzazione, oppure dopo che l'autorizzazione sia stata sospesa o revocata.

17.5. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Le regole comportamentali di carattere generale sopraindicate vengono integrate da ulteriori presidi di controllo, finalizzati a prevenire la commissione dei reati ambientali.

Di seguito vengono riportate le diverse tipologie di presidio attuate dalla Società.

Gestione dei rifiuti:

- Il servizio di raccolta, recupero, trasporto e smaltimento dei rifiuti è affidato esclusivamente a fornitori specializzati per lo svolgimento di tale attività, previa fissazione di adeguati *standard* qualitativi e verifica del possesso delle necessarie autorizzazioni previste dalla normativa di riferimento;
- Il formulario dei rifiuti viene costantemente aggiornato;
- Annualmente viene compilato e inoltrato agli organi competenti il Modello unico di dichiarazione ambientale;
- Le operazioni di recupero o smaltimento dei rifiuti sono effettuate quanto meno nel rispetto della periodicità o dei limiti quantitativi previsti dalla normativa vigente.

17.6. I controlli dell'Organismo di Vigilanza

Fermo restando il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati, commessi nell'interesse o a vantaggio della società, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

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

L'Organismo di Vigilanza dovrà, inoltre, esaminare eventuali segnalazioni specifiche provenienti dagli organi sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

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