



SILAQ SERVICE S.R.L.

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO EX D.LVO**

N. 231/2001

Revisione n. 3

Approvato dall'Organo Amministrativo in

data 11.05.2020

INDICE PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001.....	3
1.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni.....	3
1.2 L'attuazione del d. lgs. n. 231/2001	9
1.3 Destinatari del Modello.	10
1.4 Azioni da parte della società che il decreto considera esimenti dalla responsabilità amministrativa..	11
2. SANZIONI APPLICABILI	12
3. IL MODELLO ADOTTATO DA SILAQ SERVICE.....	14
3.1 Motivazioni di SILAQ SERVICE srl all'adozione del modello di organizzazione e gestione.....	14
3.2 Finalità del modello	14
3.3 Struttura del modello.....	16
3.4 Adozione, modifiche ed integrazioni del modello.....	18
3.5 Attuazione, controllo e verifica dell'efficacia del modello	19
4. IL MODELLO DI GOVERNANCE ED IL SISTEMA ORGANIZZATIVO DI SILAQ SERVICE	19
4.1 Il modello di governance di SILAQ SERVICE	19
4.2 L'assetto organizzativo di SILAQ SERVICE	20
5. IL SISTEMA DI DELEGHE E PROCURE IN SILAQ SERVICE.....	20
5.1 I principi generali.....	21
6. ORGANISMO DI VIGILANZA.....	21
6.1 Identificazione e caratteristiche dell'Organismo di Vigilanza.....	22
6.2 Funzioni e poteri dell'Organismo di Vigilanza	22
6.3 Prerogative e risorse dell'Organismo di Vigilanza.....	24
7. FLUSSI INFORMATIVI INTERNI.....	26
7.1 Reporting dell'Organismo di Vigilanza	26
7.2 Obblighi informativi nei confronti dell'Organismo di Vigilanza	27
8. FORMAZIONE E INFORMATIVA.	29
8.1 Formazione del personale	29
8.2 Diffusione del modello e del Codice Etico al personale Dirigente e Dipendente	29
8.3 Altro personale non qualificabile come dipendente.....	29
8.4 Informativa a collaboratori esterni e terze parti.....	29
9. SISTEMA DISCIPLINARE.....	30
9.1 Sanzioni applicabili ai dipendenti.....	30
9.2 Sanzioni applicabili ai Dirigenti.....	31
9.3 Disciplina applicabile nei confronti di collaboratori esterni e partners.....	32
10. VERIFICHE DELL'ODV	33
11. MODELLO E CODICE ETICO	34
12. PROCEDURA PER LA GESTIONE DI SEGNALAZIONI DI ILLECITI E MISURE A TUTELA DEL SEGNALANTE (C.D. WHISTLEBLOWER).....	34

1. IL DECRETO LEGISLATIVO N. 231/2001.

Il presente documento si prefigge di individuare le linee guida utilizzabili per la costruzione dello specifico “modello” di organizzazione, gestione e controllo di SILAQ SERVICE S.r.l., con sede legale in 20121 Milano, Piazza Castello n. 26, Codice Fiscale 08666180966, (di seguito anche “la Società” ovvero “SILAQ SERVICE”), ai sensi del D.Lgs.231/2001.

1.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni

I reati da cui può conseguire la responsabilità amministrativa per l'ente sono espressamente indicati nel D.Lgs. 231/2001, nonché in altri provvedimenti di legge che al D.Lgs. 231/2001 fanno rinvio: sono i reati contro la Pubblica Amministrazione (art. 25) e contro il suo patrimonio (art. 24); i reati informatici (art. 24 *bis*); delitti di criminalità organizzata (art. 24 *ter*); i reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 *bis*); delitti contro l'industria e il commercio (art. 25 *bis* 1); i reati societari (art. 25 *ter*); i reati con finalità di terrorismo o di eversione dall'ordine democratico (art. 25 *quater*); i reati commessi nell'effettuazione di pratiche di mutilazione degli organi genitali femminili (art. 25 *quater.1*); i reati contro la personalità individuale (art. 25 *quinquies*) ed i reati di abuso di informazioni privilegiate e di manipolazione del mercato (art. 25 *sexies*); una serie di reati (dall'associazione a delinquere, al traffico di stupefacenti, a talune fattispecie di ostacolo alla giustizia) a condizione che siano commessi da organizzazioni criminali che operano a livello internazionale (cd. reati transnazionali); reati di omicidio colposo e lesioni colpose gravissime e gravi commessi con violazione delle norme sulla sicurezza del lavoro (art. 25 *septies*); reati di ricettazione, riciclaggio e di impiego di denaro, beni o utilità di provenienza illecita nonché Cdatoriciclaggio (art. 25 *octies*); delitti in materia di violazione del diritto d'Cdatore (art. 25 *nonies*); induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Cdatorità giudiziaria (art. 25 *decies*), i reati ambientali (art. 25 *undecies*), inosservanza delle sanzioni interdittive (art. 23); impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies*); corruzione tra privati (art. 25-*ter*, comma 1, lettera s-*bis*).

Il Decreto n. 231 inizialmente prevedeva i soli reati contemplati nelle norme di cui agli artt. 24 e 25: per effetto di provvedimenti normativi successivi la casistica dei reati si è tuttavia notevolmente ampliata. Questo l'insieme dei reati attualmente richiamati dal D.Lgs. 231/2001, o normative che ad esso fanno rinvio, da cui consegue la responsabilità amministrativa dell'ente:

1) 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 (Artt. 24 e 25 D. Lgs. 231/2001, mod. dalla L. 161/2017)):

- indebita percezione di erogazioni a danno dello Stato o di altro ente pubblico (art. 316 *ter* c.p.);
- malversazione a danno dello Stato o di altro ente pubblico (art. 316 *bis* c.p.);
- truffa in danno dello Stato o di un ente pubblico (art. 640 comma 2 n. 1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.);

- frode informatica a danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.);
- corruzione (artt. 318, 319, 320, 321 e 322 *bis* c.p.);
- istigazione alla corruzione (322 c.p.);
- corruzione in atti giudiziari (319 *ter* c.p.);
- concussione (art. 317 c.p.);
- induzione indebita a dare o promettere utilità (art. 319 *quater* c.p.).

2) Reati informatici (art. 24 *bis*):

- Falsità in documenti informatici (art. 491 *bis* c.p.);
- 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 e telematico (art. 615 *quinquies* c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);
- 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.);
- Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.);
- Frode informatica con sostituzione dell'identità digitale (art. 640 *ter* comma 3 c.p.).

3) Delitti di criminalità organizzata (art. 24 *ter*):

- associazione per delinquere (art. 416 c.p.);
- associazioni di tipo mafioso anche straniere (art. 416 *bis* c.p.);
- scambio elettorale politico mafioso (art. 416 *ter* c.p.);
- sequestro di persona a scopo di estorsione (art. 630 c.p.).

4) Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 *bis*):

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- alterazione di monete (art. 454 c.p.);
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);

- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- uso di valori di bollo contraffatti o alterati (art. 464 commi 1 e 2 c.p.);
- falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

5) Delitti contro l'industria e il commercio (art. 25 bis 1):

- turbata libertà dell'industria o del commercio (art. 513 c.p.);
- illecita concorrenza con minaccia o violenza (art. 513 bis c.p.);
- frodi contro le industrie nazionali (art. 514 c.p.);
- frode nell'esercizio del commercio (art. 515 c.p.);
- vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.).

6) Reati societari (art. 25 ter):

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622 commi 1 e 3 c.c.);
- impedito controllo (art. 2625 comma 2 c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggio (art. 2637 c.c.);
- omessa comunicazione del conflitto d'interessi (art. 2629 bis c.c.);
- ostacolo all'esercizio delle funzioni delle Cdatorità pubbliche di vigilanza (art. 2638 commi 1 e 2 c.c.).

7) Reati commessi con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater);

8) Reati commessi nell'effettuazione di pratiche di mutilazione degli organi genitali femminili (art. 25 quater);

9) Reati contro la personalità individuale (art. 25 quinquies):

- riduzione in schiavitù (art. 600 c.p.);
- tratta e commercio di schiavi (art. 601 c.p.);
- alienazione e acquisto di schiavi (art. 602 c.p.);

- prostituzione minorile (art. 600 *bis* commi 1 e 2 c.p.);
- pornografia minorile (art. 600 *ter* c.p.);
- iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 *quinquies* c.p.);
- detenzione di materiale pornografico (art. 600 *quater* c.p.).

10) Reati di abuso di mercato (art. 25 *sexies*):

- Abuso di informazioni privilegiate (art. 184 T.U.F. D.Lgs. 24.2.1998 n. 58);
- Manipolazione del mercato (art. 185 T.U.F. D.Lgs. 24.2.1998 n. 58).

11) Reati in materia di tutela della salute e della sicurezza dei lavoratori commessi con violazione delle norme antinfortunistiche (art. 25 *septies*, introdotto dalla Legge 3.8.2007 n. 123 recante “Misure in tema di tutela della salute e della sicurezza sul lavoro”, entrata in vigore il 25.8.2007 e sostituita dal D.Lgs. 81/2008 “T.U. Sicurezza e salute sui luoghi di lavoro”):

- Omicidio colposo (art. 589 c.p.);
- Lesioni colpose gravi o gravissime (art. 590 comma terzo c.p.).

12) Reati di ricettazione, riciclaggio e impiego di beni di provenienza illecita nonché Cdatoriciclaggio (art. 25 *octies*):

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648 *bis* c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 *ter* c.p.);
- Cdatoriciclaggio (art. 648 *ter.1* c.p.).

13) Delitti in materia di violazione del diritto d’Cdatore (art. 171 primo comma, lettera a bis e terzo comma, art. 171 bis, art. 171 ter, art. 171 *octies* Legge 22 aprile 1941 n° 633) – art. 25 *nonies*;

14) Reati transnazionali (Legge 16.3.06 n. 146):

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416 *bis* c.p.);
- Associazione finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 *quater* Legge 92/2001);
- Associazione finalizzata al traffico di sostanze stupefacenti (art. 74 DPR 09/10/90 n° 309);
- Traffico di migranti;
- Favoreggiamento personale (art. 378 c.p.).

15) Induzione a rendere dichiarazioni mendaci all’Cdatorità Giudiziaria (377 *bis* c.p.) - art. 25 *decies*;

16) Reati ambientali (art. 25 *undecies*)

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari appartenenti ad una specie animale e/o vegetale selvatica protetta (c.p. art. 727 *bis*);

- Distruzione o deterioramento di habitat all'interno di un sito protetto (c.p. art. 733 *bis*);
- Scarico di acque reflue industriali contenenti sostanze pericolose (D.Lgs. 152/06 art. 137 comma 1);
- Scarico di acque reflue industriali contenenti sostanze pericolose in violazione delle prescrizioni imposte con l' Cdatorizzazione o dalle Cdatorità competenti (D.Lgs. 152/06 art. 132, comma 2);
- Scarico di acque reflue industriali contenenti sostanze pericolose in violazione dei limiti tabellari o dei limiti più restrittivi fissati da Regioni o Province Cdatonome o dall' Cdatorità competente (D.Lgs. 152/06 art.137, comma 5, primo e secondo periodo);
- Violazione dei divieti di scarico al suolo, nelle acque sotterranee, nel suolo o nel sottosuolo (D.Lgs. 152/06 art.137, comma 11);
- Scarico in mare da parte di navi o aeromobili di sostanze o materiali di cui è vietato lo sversamento, salvo in quantità minime e Cdatorizzato dall' Cdatorità competente (D.Lgs. 152/06 art. 137, comma 13);
- Attività di gestione di rifiuti non Cdatorizzata (D.Lgs. 152/06 art.256, comma 1);
- Realizzazione o gestione di discarica non Cdatorizzata (D.Lgs. 152/06 art. 256, comma 3, primo periodo);
- Realizzazione o gestione di discarica non Cdatorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi (D.Lgs. 152/06 art. 256, comma 3, secondo periodo);
- Attività non consentita di miscelazione di rifiuti (D.Lgs. 152/06 art. 256, comma 5);
- Deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi (D.Lgs. 152/06 art.256, comma 6);
- Omessa bonifica (D.Lgs. 152/06 art. 257);
- Predisposizione di un certificato di analisi dei rifiuti falso e uso del certificato durante il trasporto (D.Lgs. 152/06 art. 258, comma 4);
- Predisposizione di un certificato di rifiuti falso, utilizzato nell'ambito del sistema di tracciabilità SISTRI (D.Lgs. 152/06, art. 260 *bis*, comma 6);
- Trasporto di rifiuti pericolosi senza la copia cartacea della scheda SISTRI-AREA MOVIMENTAZIONE o senza certificato analitico dei rifiuti, nonché uso di certificato di analisi contenente informazioni false circa i rifiuti trasportati in ambito SISTRI (D.Lgs. 152/06, art. 260 bis comma 7, secondo periodo e terzo periodo);
- Trasporto di rifiuti con copia cartacea della scheda SISTRI-AREA MOVIMENTAZIONE frCdadolentemente alterata (D.Lgs. 152/06, art. 260 bis comma 8, primo e secondo periodo);
- Traffico illecito di rifiuti (D.Lgs. 152/06, art. 259);
- Attività organizzate per il traffico illecito di rifiuti (D.Lgs. 152/06, art. 260);
- Violazione, nell'esercizio di uno stabilimento, dei valori limite di emissione o delle prescrizioni stabilite dall' Cdatorizzazione, dai piani e programmi o dalla normativa, ovvero dall' Cdatorità competente, che determini anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa (D.Lgs. 152/06, art. 279, comma 5);
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L.150/92, art. 1 e art. 2);
- Falsificazione o alterazione di certificati e licenze; notifiche, comunicazioni o dichiarazioni false o alterate al fine di acquisire un certificato o una licenza; uso di certificati e licenze falsi o alterati per l'importazione di animali (L. 150/92, art. 3 bis, comma 1);
- Detenzione di esemplari vivi di mammiferi e rettili di specie selvatica o riprodotti in cattività, che costituiscono pericolo per la salute e per l'incolumità pubblica (L. 150/92, art. 6, comma 4);

- Violazione delle disposizioni che prevedono la cessazione e la riduzione dell'impiego (produzione, utilizzazione, commercializzazione, importazione ed esportazione) di sostanze nocive per lo strato di ozono (Legge n° 549 del 1993, art. 3, comma 6);
- Sversamento doloso in mare di sostanze inquinanti (D.Lgs. 202/07, art. 8);
- Sversamento colposo in mare di sostanze inquinanti (D.Lgs. 202/07, art. 9).

17) Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 22 comma 12 *bis* D.Lgs. 286/1998) - art. 25 *duodecies*;

18) Corruzione tra privati (art. 2635 c.c.) – art. 25 *ter*, comma 1, lettera s.

Pare opportuno precisare che i reati ora elencati nel par. 14 possono determinare la responsabilità dell'Ente alla sola condizione che siano connotati dal carattere della "transnazionalità". Per potersi definire transnazionale il reato deve essere stato commesso da un gruppo criminale organizzato e deve altresì ricorrere una delle seguenti circostanze:

- che il reato sia commesso in più di uno Stato;
- che il reato sia commesso in uno Stato ma una parte della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- che il reato sia commesso in uno Stato ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- che il reato sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

In assenza dei suddetti requisiti le sanzioni derivanti dalla commissione dei reati anzidetti continueranno a riguardare solo le persone fisiche che li hanno commessi.

19) Razzismo e xenofobia (Art. 25-*terdecies*)

- Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale (Art. 3, comma 3-bis della Legge 654/1975) - articolo abrogato dal D.Lgs. n. 21/2018 e sostituito dall'art. 604 bis c.p.
- Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 604 bis)

20) Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013)

21) Reati tributari (Art. 25-*quinquedecies* | D. Lgs. 231/01)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Dichiarazione fraudolenta mediante altri artifici (Art. 3 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Dichiarazione infedele (Art. 4 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Omessa dichiarazione (Art.5 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Emissione di fatture o altri documenti per operazioni inesistenti (Art.8 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)

- Occultamento o distruzione di documenti contabili (Art.10 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Sottrazione fraudolenta al pagamento di imposte (Art.11 D.Lgs 74 e s.m.)
- Casi particolari di confisca (Art.12-ter aggiunto dall' art. 39 del D.L. 124 del 26 ottobre 2019)

SILAQ SERVICE, a seguito delle verifiche sull'attività aziendale, ha ritenuto estremamente improbabile la commissione dei reati di seguito elencati.

- Delitti di criminalità organizzata (art. 24 ter);
- Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis);
- Delitti contro l'industria e il commercio (art. 25 bis 1);
- Reati commessi con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 *quater*);
- Reati commessi nell'effettuazione di pratiche di mutilazione degli organi genitali femminili (art. 25 *quater*);
- Reati contro la personalità individuale (art. 25 *quinquies*);
- Reati di abuso di mercato (art. 25 *sexies*);
- Reati di ricettazione, riciclaggio e impiego di beni di provenienza illecita nonché di riciclaggio (art. 25 *octies*);
- Delitti in materia di violazione del diritto d'autore (art. 171 primo comma, lettera a bis e terzo comma, art. 171 bis, art. 171 ter, art. 171 *octies* Legge 22 aprile 1941 n° 633) – art. 25 *nonies*;
- Reati transnazionali (Legge 16.3.06 n. 146);
- Induzione a rendere dichiarazioni mendaci all'autorità Giudiziaria (377 *bis* c.p.) - art. 25 *decies*;
- Reati ambientali (art. 25 *undecies*);
- Corruzione tra privati (art. 2635 c.c.) – art. 25 *ter*, comma 1, lettera s;
- Razzismo e xenofobia (Art. 25-*terdecies*);
- Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013).

1.2 L'attuazione del d. lgs. n. 231/2001

L'adozione del Modello è, per legge, facoltativa. Tuttavia, che si tratti di uno strumento organizzativo irrinunciabile appare evidente in considerazione della centrale funzione di esclusione della responsabilità dell'ente che la legge gli riconosce.

Tale funzione è subordinata all'effettiva idoneità del modello da valutarsi nella duplice fase della preventiva adozione e successiva attuazione. Il giudice penale dovrà, cioè, valutare sia l'idoneità del documento a svolgere la funzione di prevenzione affidatagli dalla legge, sia l'effettività delle modalità concrete con cui esso è reso operativo all'interno dell'ente.

Sempre sul piano della funzione svolta, i modelli esplicano effetti differenti in relazione al ruolo che l'autore del reato riveste nel contesto organizzativo dell'ente: nel caso di reato commesso da soggetti in posizione apicale, il modello organizzativo dovrà essere strutturato in modo da prevenire illeciti suscettibili di essere realizzati nella fase di formazione ed attuazione delle decisioni dell'ente; diversamente, nella

situazione in cui responsabile sia un dipendente sottoposto all'altrui vigilanza il modello dovrà risultare efficace rispetto al differente momento dell'esecuzione delle decisioni stesse.

Il Modello può avere come riferimento, oltre alle prescrizioni del Decreto, le Linee Guida elaborate in materia da associazioni di categoria.

In attuazione di quanto previsto dal Decreto, gli organi competenti all'adozione del Modello, devono affidare ad un organo *ad hoc* l'incarico di assumere le funzioni di Organo di vigilanza (di seguito ODV) con Cdtonomi compiti di vigilanza, controllo e iniziativa in relazione al Modello stesso.

1.3 Destinatari del Modello.

I destinatari delle norme e delle prescrizioni contenute nel Modello sono tutti gli esponenti dell'ente collettivo: lavoratori, dirigenti, amministratori e membri degli altri organi sociali; altresì destinatari del Modello - tenuti, quindi, al suo rispetto - sono i collaboratori esterni, i liberi professionisti, i consulenti (collettivamente, "Collaboratori Esterni") nonché tutti i *partners* commerciali ("Partners").

Il ruolo di SILAQ SERVICE S.r.l. si esplica inoltre in attività di informazione e gestione delle relazioni con i clienti, costituiti da società e professionisti sul territorio italiano.

SILAQ SERVICE s.r.l. è inoltre il gestore di servizi per le società client, mette cioè a disposizione sulla base di un contratto per prestazione di servizi retribuiti – servizi di consulenza, assistenza e supporto nelle seguenti aree:

- preparazione dei bilanci e tenuta della contabilità, revisione delle modalità di controllo interne e rispetto delle procedure contabili globali applicabili;
- questioni amministrative varie su richiesta delle società clienti;
- organizzazione ed erogazione di corsi di formazione;

Tali servizi possono essere forniti direttamente da SILAQ SERVICE S.r.l. o in alcuni casi dalla stessa procurati e forniti attraverso consulenti o professionisti esterni.

1.4 Azioni da parte della società che il decreto considera esimenti dalla responsabilità amministrativa

L'articolo 6 del Decreto prevede una forma specifica di esimente dalla responsabilità amministrativa qualora l'Ente dimostri che:

- a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto illecito, modelli di organizzazione e gestione idonei a prevenire la realizzazione degli illeciti penali considerati;
- b) ha affidato ad un organo interno, l'ODV, dotato di Cdautonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'efficace osservanza del modello in questione, nonché di curarne l'aggiornamento;
- c) le persone che hanno commesso il reato hanno agito eludendo frCdadolentemente il Modello su indicato;
- d) non vi è stato omesso o insufficiente controllo da parte dell'ODV.

Al comma 2 del medesimo art.6, il Decreto prevede inoltre che i modelli di organizzazione e gestione debbano rispondere alle seguenti esigenze:

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

La formulazione dei modelli e l'organizzazione dell'attività dell'ODV devono porsi l'**obiettivo del giudizio di idoneità**, da parte dell'Cdatorità giudiziaria, che conduca all'esonero di responsabilità dell'ente. A tale proposito lo stesso Decreto prevede che i modelli di organizzazione e di gestione, garantendo le esigenze suddette, possono essere adottati sulla base di codici di comportamento (c.d. Linee Guida) redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia, che – di concerto con i Ministeri competenti – può formulare entro trenta giorni osservazioni sulla idoneità dei modelli di organizzazione e di gestione a prevenire i reati.

2. SANZIONI APPLICABILI.

Nell'ipotesi in cui i soggetti di cui all'art. 5 del Decreto commettano uno dei reati previsti dagli artt. 24 e ss. del Decreto o di quelli previsti dalla normativa speciale richiamata, l'Ente potrà subire l'irrogazione di pesanti sanzioni.

A mente dell'art. 9, le sanzioni, denominate *amministrative*, si distinguono in:

- I. sanzioni pecuniarie;
- II. sanzioni interdittive;
- III. confisca;
- IV. pubblicazione della sentenza.

Dal punto di vista generale, è opportuno precisare che l'accertamento della responsabilità dell'Ente, nonché la determinazione dell'*an* e del *quantum* della sanzione, sono attribuiti al Giudice penale competente per il procedimento relativo ai reati dai quali dipende la responsabilità amministrativa.

L'Ente è ritenuto responsabile dei reati individuati dagli artt. 24 e ss. anche se questi siano stati realizzati nelle forme del tentativo. In tali casi, però, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà.

L'Ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

I. Le sanzioni pecuniarie

Le sanzioni pecuniarie trovano regolamentazione negli artt. 10, 11 e 12 del Decreto e si applicano in tutti i casi in cui sia riconosciuta la responsabilità dell'Ente. Le sanzioni pecuniarie vengono applicate per "quote", in numero non inferiore a 100 e non superiore a mille, mentre l'importo di ciascuna quota va da un minimo di € 258,23 ad un massimo di € 1.549,37. Il Giudice determina il numero di quote sulla base degli indici individuati dal I comma dell'art. 11, mentre l'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente coinvolto.

II. Le sanzioni interdittive

Le sanzioni interdittive, individuate dal comma II dell'art. 9 del Decreto ed irrogabili nelle sole ipotesi tassativamente previste e solo per alcuni dei reati, sono:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle Cdatorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

e) il divieto di pubblicizzare beni e servizi.

Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinati dal Giudice penale che conosce del processo per i reati commessi dalle persone fisiche, tenendo conto dei fattori meglio specificati dall'art. 14 del Decreto. In ogni caso, le sanzioni interdittive hanno una durata minima di tre mesi e massima di due anni.

Uno degli aspetti di maggiore interesse è che le sanzioni interdittive possono essere applicate all'Ente sia all'esito del giudizio e, quindi, accertata la colpevolezza dello stesso, sia in via cautelare, ovvero quando vi siano:

- gravi indizi per ritenere la sussistenza della responsabilità dell'Ente per un illecito amministrativo dipendente da reato;
- fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

III. La confisca

La confisca del prezzo o del profitto del reato è una sanzione obbligatoria che consegue alla eventuale sentenza di condanna (art. 19). Occorre, inoltre, tenere presente che l'art. 31 della legge n. 34/2008 (cosiddetta "Comunitaria 2008") delega il Governo ad ampliare notevolmente la portata applicativa dell'art. 19 del Decreto.

IV. La pubblicazione della sentenza

La pubblicazione della sentenza è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva (art. 18).

3. IL MODELLO ADOTTATO DA SILAQ SERVICE.

3.1 Motivazioni di SILAQ SERVICE srl all'adozione del modello di organizzazione e gestione

SILAQ SERVICE è una società italiana che svolge attività di consulenza in materia preparazione dei bilanci e tenuta della contabilità; revisione delle modalità di controllo interne e rispetto delle procedure contabili globali applicabili; questioni amministrative varie su richiesta delle società clienti; organizzazione ed erogazione di corsi di formazione.

SILAQ SERVICE ha ritenuto necessario adottare un modello di organizzazione e di gestione in linea con le prescrizioni del Decreto (di seguito “Modello”).

SILAQ SERVICE ritiene che l'adozione di tale Modello, unitamente alla emanazione del Codice Etico, costituiscano, al di là delle prescrizioni di legge, un ulteriore valido strumento di sensibilizzazione di tutti i dipendenti di SILAQ SERVICE e di tutti gli altri soggetti alla stessa cointeressati (Fornitori, Committenti, Terze Parti, ecc.). Tutto ciò affinché i suddetti soggetti seguano, nell'espletamento delle proprie attività, comportamenti corretti, sicuri e trasparenti tali da prevenire il rischio di commissione dei reati contemplati dal Decreto.

SILAQ SERVICE ha predisposto il Modello sulla base di quanto previsto dal Decreto e dalle Linee Guida formulate da Confindustria.

In attuazione di quanto previsto dal Decreto, il Cda di SILAQ SERVICE, nell'approvare il Modello, ha affidato ad un apposito organismo monocratico (composto da un consulente esterno) l'incarico di assumere le funzioni di ODV, con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento. Per quanto concerne i dettagli in merito all'ODV nominato dalla Società si veda il punto 5 del presente Modello.

3.2 Finalità del modello

Il Modello predisposto da SILAQ SERVICE si fonda su di un complesso, strutturato ed organico, di procedure e controlli finalizzati al presidio delle attività aziendali maggiormente esposte, anche solo potenzialmente, alla verifica dei reati (aree a rischio) contemplati dal Decreto, per prevenirne od impedirne la commissione. Tale sistema di procedure e attività di controllo nella sostanza:

- a) individuano le aree/i processi di possibili rischi nella attività aziendale, con particolare riguardo a quelle che comportano un rischio reato ai sensi del Decreto, ne valutano l'impatto economico, lo verificano e lo documentano (*Risk Mapping & Management*);
- b) definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni di SILAQ SERVICE in relazione ai rischi/reati da prevenire tramite:
 - I) un sistema normativo – composto dal Codice Etico della Società - che fissa le linee di orientamento generali, formalizzate nel tempo, tese a disciplinare in dettaglio le modalità per assumere ed attuare decisioni nei settori “sensibili”;
 - II) un sistema di deleghe e di poteri aziendali che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni;
 - III) la definizione di strutture organizzative coerenti ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti dalla struttura organizzativa siano realmente attuati;
- c) individuano i processi di gestione e controllo delle risorse finanziarie nelle attività potenzialmente a rischio reato;
- d) attribuiscono ad un ODV specifici compiti di vigilanza sull'efficacia e corretto funzionamento del Modello, sulla coerenza dello stesso con gli obiettivi e sul suo aggiornamento periodico.

Le **finalità del Modello** sono pertanto quelle di:

- a) prevenire e ragionevolmente limitare i possibili rischi connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali condotte illecite;
- b) determinare, in tutti coloro che operano in nome e per conto di SILAQ SERVICE, nelle aree di attività a rischio, la consapevolezza di poter incorrere, nel caso di violazioni alle disposizioni riportate nel Modello, in un reato passibile di sanzioni penali e amministrative non solo nei loro confronti, ma anche nei confronti di SILAQ SERVICE;
- c) ribadire che SILAQ SERVICE non tollera comportamenti illeciti, di ogni tipo e indipendentemente da qualsiasi finalità, in quanto gli stessi, oltre a trasgredire le leggi vigenti, sono comunque contrari ai principi etico-sociali cui SILAQ SERVICE intende attenersi.

Spostandosi dallo specifico contesto operativo di SILAQ SERVICE, sia interno che esterno, il Modello rappresenta il risultato dell'applicazione metodologica documentata dei criteri di identificazione dei rischi, da un lato, e di individuazione dei protocolli per la programmazione, la formazione e l'attuazione delle decisioni della società, dall'altro.

Nell'ottica di un processo di adeguamento continuo ai mutamenti societari, alle esigenze in divenire del mercato ed alla evoluzione normativa di riferimento, il Modello è volto ad imporre un sistema compatibile con la struttura societaria, così da integrarsi efficientemente con l'operatività aziendale, ma nello stesso tempo fermamente rivolto al perseguimento dei rigorosi principi finalistici che lo animano.

Il Modello si prefigge, infatti, di indurre tutti i Destinatari, quale che sia il rapporto, anche temporaneo, che li lega a SILAQ SERVICE, ad acquisire la sensibilità necessaria per percepire la sussistenza dei rischi di commissione di reati nell'esercizio di determinate attività ed insieme comprendere la portata, non solo personale ma anche societaria, delle possibili conseguenze connesse, in termini di sanzioni penali ed amministrative.

A tal fine la società si propone, con l'adozione del Modello, di conseguire il pieno e consapevole rispetto dei principi su cui lo stesso si fonda, così da impedirne l'elusione fraudolenta e, nel contempo, contrastare fortemente tutte quelle condotte che siano contrarie alle disposizioni di legge ed al Codice Etico di SILAQ SERVICE.

3.3 Struttura del modello

Il Modello si compone di una "Parte Generale" e di singole "Parti Speciali" predisposte per le differenti tipologie di reati contemplate dal Decreto.

L'articolazione del Modello in una "Parte Generale" ed in più "Parti Speciali" è finalizzata a garantire una più efficace e snella attività di aggiornamento dello stesso. Infatti, se la "Parte Generale" contiene la formulazione di principi di diritto da ritenersi sostanzialmente costanti, le diverse "Parti Speciali", in considerazione del loro particolare contenuto, sono suscettibili invece di costanti aggiornamenti. Inoltre, l'evoluzione legislativa – quale ad esempio una possibile estensione delle tipologie di reati che, per effetto di altre normative, risultino inserite o comunque collegate all'ambito di applicazione del Decreto – potrà rendere necessario l'integrazione del Modello con ulteriori "Parti Speciali".

In particolare, la Parte Speciale è attualmente suddivisa nelle seguenti parti:

- la "Parte Speciale A" relativa ai reati nei confronti della Pubblica Amministrazione;
- la "Parte Speciale B" relativa ai reati societari;
- la "Parte Speciale C" relativa ai reati in tema di salute e sicurezza sul lavoro;
- la "Parte Speciale D" relativa ai reati contro il patrimonio;
- la "Parte Speciale E" relativa ai reati informatici;

- la “Parte Speciale F” relativa ai reati in tema di assunzione di lavoratori stranieri (ex art. 22 comma 12 *bis* D.Lgs. 286/1998 - art. 25 *duodecies*);
- la “Parte Speciale G” relativa alle check list per le verifiche.
- la “Parte speciale H” relativa alle check list per le verifiche.

Nell’ambito delle Parti Speciali, sono stati indicati:

- le aree ritenute “a rischio reato” e le attività sensibili;
- i reati astrattamente perpetrabili;
- le aree ritenute “strumentali”, nonché i soggetti che in esse agiscono;
- la tipologia dei controlli in essere sulle singole aree di rischio e strumentali
- i principi di comportamento da rispettare al fine di ridurre il rischio di commissione dei reati;
- i compiti spettanti all’OdV al fine di prevenire il pericolo di commissione dei reati.

SILAQ SERVICE si riserva, comunque, di valutare l’opportunità di procedere alla predisposizione di ulteriori parti speciali relative ad altre fattispecie di reato già contemplate dal Decreto.

Il presente Modello è, inoltre, accompagnato da alcuni allegati (organigramma aziendale, schema riassuntivo sistema deleghe e procure) nonché dai documenti che, rappresentativi di alcuni protocolli, completano e specificano il quadro della organizzazione, della gestione e del controllo della Società, quali il Codice Etico ed il Sistema Disciplinare, oltre che il Documento di valutazione dei rischi, il Documento Programmatico sulla Sicurezza ed il Manuale Privacy. Tali documenti, unitariamente considerati, costituiscono il Modello della Società adottato ai sensi del Decreto.

Al di là delle descritte procedure, che operano *ex ante*, saranno comunque sempre possibili verifiche successive su singole operazioni o singoli comportamenti aziendali (controllo *ex post*).

Le procedure e le misure adottate non potranno mai dirsi definitive: la loro efficacia e completezza dovrà, al contrario, essere oggetto di continua valutazione e dovranno essere immediatamente proposti e realizzati i miglioramenti, le integrazioni e le modifiche che si renderanno di volta in volta necessarie.

SILAQ SERVICE ha inteso dotarsi di un **sistema organizzativo adeguatamente formalizzato e rigoroso nell’attribuzione delle responsabilità, linee di dipendenza gerarchica e puntuale descrizione dei ruoli, con assegnazione di poteri Cdatorizzativi e di firma coerenti con responsabilità definite, nonché con predisposizione di meccanismi di controllo fondati sulla contrapposizione funzionale e separazione dei compiti.** Tale organizzazione di poteri e responsabilità risulta anche dai documenti di gestione aziendali attualmente in atto e sarà ulteriormente definita dalle delibere e dagli altri atti di attuazione del presente Modello.

L'applicazione del Modello viene garantita anche mediante la definizione di regole generali e di idonee procedure per disciplinare i processi delle diverse aree aziendali, soprattutto quelle a maggior rischio di commissione dei reati, nonché da un adeguato sistema disciplinare.

SILAQ SERVICE ha, inoltre, individuato un sistema di controllo di gestione basato su strumenti consolidati nella pratica amministrativa che consenta la tempestiva rilevazione dell'insorgenza ed esistenza di anomalie e criticità da gestire ed annullare.

Soprattutto, ma non solo, nell'area della gestione finanziaria, SILAQ SERVICE si avvale e si avvarrà di un efficiente sistema informativo, caratterizzato da procedure manuali ed informatiche in grado di consentire che ogni operazione risulti adeguatamente supportata sul piano documentale così da poter procedere in qualsiasi momento all'esecuzione di controlli che individuino finalità e motivazioni dell'operazione con identificazione del ciclo completo di Cdatorizzazione, registrazione e verifica dell'operazione stessa.

Infine, il Modello prevede un impianto di informazione, connesso ad un coerente programma di formazione, che permetta di far raggiungere a tutti i Destinatari che operano per l'azienda il flusso aggiornato delle comunicazioni societarie di natura organizzativa, gestionale, normativa ed etica necessarie per il corretto funzionamento della società e del Modello.

In considerazione di quanto sopra, l'ODV provvederà ad richiedere simili aggiornamenti ed integrazioni delle singole "Parti Speciali".

3.4 Adozione, modifiche ed integrazioni del modello

Ai sensi dell'art. 6, lett. a) del Decreto 231/01, l'adozione del Modello è atto di emanazione dell'organo dirigente, che provvederà ad integrarlo ed aggiornarlo in considerazione di sopravvenute modifiche normative o di esigenze palesate dall'attuazione dello stesso.

Pertanto, adottato il Modello con delibera dell'Cda di SILAQ SERVICE (di seguito CDA), anche le successive modifiche ed integrazioni di carattere sostanziale del Modello, che dovessero rendersi necessarie per sopravvenute esigenze aziendali ovvero per adeguamenti normativi, sono di competenza del medesimo organo amministrativo.

E' attribuito all'ODV il potere di proporre modifiche al Modello o integrazioni di carattere formale nonché quelle modifiche ed integrazioni del Modello consistenti nella:

- I) introduzione di nuove procedure e controlli nel caso in cui non sia sufficiente una revisione di quelle esistenti;

- II) revisione dei documenti aziendali e societari che formalizzano l'attribuzione delle responsabilità e dei compiti alle posizioni responsabili di strutture organizzative "sensibili" o comunque che svolgono un ruolo di snodo nelle attività a rischio;
- III) introduzione di ulteriori controlli delle attività sensibili, con formalizzazione delle iniziative di miglioramento intraprese in apposite procedure;
- IV) evidenziazione delle esigenze di integrare regole di carattere generale restando poi comunque necessaria l'approvazione del Modello con delibera dell'CDA.

3.5 Attuazione, controllo e verifica dell'efficacia del modello

L'attuazione del Modello è rimessa alla responsabilità di SILAQ SERVICE; sarà compito specifico dell'ODV verificare e controllare l'effettiva ed idonea applicazione del medesimo in relazione alle specifiche attività aziendali.

Quindi, ferma restando la responsabilità dell'CDA riguardo all'attuazione del Modello, si intende attribuito all'ODV il compito di coordinare le previste attività di controllo e di raccogliere e sintetizzarne i risultati.

4. IL MODELLO DI GOVERNANCE ED IL SISTEMA ORGANIZZATIVO DI SILAQ SERVICE

Il modello di *governance* di SILAQ SERVICE e, in generale, tutto il suo sistema organizzativo, è interamente strutturato in modo da assicurare alla Società l'attuazione delle strategie ed il raggiungimento degli obiettivi.

La struttura di SILAQ SERVICE, infatti, è stata creata tenendo conto della necessità di dotare la Società di una organizzazione tale da garantirle la massima efficienza ed efficacia operativa.

4.1 Il modello di governance di SILAQ SERVICE

Il sistema di *corporate governance* di SILAQ SERVICE risulta così articolato:

- Assemblea:

L'assemblea dei Soci è competente a deliberare, in sede ordinaria e straordinaria, sulle materie alla stessa riservate dalla Legge o dallo Statuto.

- Cda:

L'Cda è investito dei più ampi poteri per l'amministrazione della Società e per l'attuazione ed il raggiungimento dello scopo sociale, nei limiti di quanto consentito dalla legge e dallo Statuto. All'Cda risulta quindi, tra l'altro, conferito il potere di definire gli indirizzi strategici della Società, di verificare l'esistenza e l'efficienza dell'assetto organizzativo ed amministrativo della Società.

Al momento dell'adozione del presente Documento, il capitale sociale della Società è interamente detenuto

da Ricerche, Studi e Consulenze Company S.r.l.

4.2 L'assetto organizzativo di SILAQ SERVICE

La struttura organizzativa della Società è orientata a garantire, da un lato, la separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, dall'altro, la massima efficienza possibile.

In particolare, la struttura organizzativa aziendale, che è improntata ad una precisa definizione delle competenze di ciascuna Area aziendale e delle connesse responsabilità, è articolata secondo il seguente organigramma, i cui eventuali aggiornamenti saranno disponibili presso la Direzione Risorse umane.

4.2.1. I comitati interni

Nell'ambito della struttura organizzativa di SILAQ SERVICE potrà essere istituito un comitato interno denominato Management Team, che si occuperà di monitorare e gestire tutte le attività attinenti la gestione operativa della società.

4.2.2. Le *Company Policies* e le Procedure Operative Standard

Nella prospettiva di un'efficace implementazione del Modello, particolare rilievo assume l'integrazione dei Protocolli della Parte Speciale con le procedure adottate in ambito societario.

SILAQ SERVICE ha adottato una serie di *Company Policies* che disciplinano varie aree dell'attività svolta; gli *standards* di condotta professionale ed etica stabiliti da tali politiche aziendali sono validi per tutti i dipendenti di SILAQ SERVICE. Dunque, anche SILAQ SERVICE ha adottato le *policies* aziendali di seguito indicate, che rilevano in questa sede a completamento delle prescrizioni della Parte Generale a che vengono allegate al presente modello.

Le più rilevanti Politiche Aziendali in questo senso sono le seguenti:

- Codice di Condotta professionale ed Etica di SILAQ SERVICE
- General Compliance Policy
- Politica per le attività Promozionali
- Ospitalità, Intrattenimento e Doni
- Condotta professionale con impiegati pubblici e governativi
- *IT Policy* adottata nella società e denominata "Regolamento sul sistema informativo aziendale e uso degli strumenti".

5. IL SISTEMA DI DELEGHE E PROCURE IN SILAQ SERVICE

5.1 I principi generali

Così come richiesto dalla buona pratica aziendale e specificato anche nelle Linee Guida di Confindustria, il Cda di SILAQ SERVICE è l'organo preposto a conferire ed approvare formalmente le deleghe ed i poteri di firma, assegnati in coerenza con le responsabilità organizzative e gestionali definite e prevedendo una puntuale indicazione delle soglie di approvazione delle spese.

Il livello di Cdautonomia, il potere di rappresentanza ed i limiti di spesa assegnati ai vari titolari di deleghe e procure all'interno della Società risultano sempre individuati e fissati in stretta coerenza con il livello gerarchico del destinatario della delega o della procura.

I poteri così conferiti vengono periodicamente aggiornati in funzione dei cambiamenti organizzativi intervenuti nella struttura della Società.

La Società ha, inoltre, istituito un flusso informativo, nei confronti di tutte le funzioni e soggetti aziendali, a qualsiasi titolo interessati (incluso l'OdV), al fine di garantire la tempestiva comunicazione dei poteri e dei relativi cambiamenti.

Ciascuno di questi atti di delega o conferimento di poteri di firma fornisce le seguenti indicazioni:

- 1) soggetto delegante e fonte del suo potere di delega o procura;
- 2) soggetto delegato, con esplicito riferimento alla funzione ad esso attribuita ed il legame tra le deleghe e le procure conferite e la posizione organizzativa ricoperta dal soggetto delegato;
- 3) oggetto, costituito dalla elencazione delle tipologie di attività e di atti per i quali la delega/procura viene conferita. Tali attività ed atti sono sempre funzionali e/o strettamente correlati alle competenze e funzioni del soggetto delegato;
- 4) limiti di valore entro cui il delegato è legittimato ad esercitare il potere conferitogli. Tale limite di valore è determinato in funzione del ruolo e della posizione ricoperta dal delegato nell'ambito dell'organizzazione aziendale.

Le deleghe e le procure in SILAQ SERVICE, oltre ad essere pubblicizzate attraverso specifici canali di comunicazione, vengono raccolte, organizzate secondo la struttura aziendale a cui corrispondono e sono poste sempre a disposizione anche di tutti gli altri soggetti aziendali, ovvero di terzi interessati, presso la sede della Società.

Il sistema delle deleghe e dei poteri di firma, come sopra delineato, è costantemente applicato nonchè regolarmente e periodicamente monitorato nel suo complesso e, ove del caso, aggiornato in ragione delle modifiche intervenute nella struttura aziendale, in modo da corrispondere e risultare il più possibile coerente con l'organizzazione gerarchico-funzionale della Società. Sono attuati singoli aggiornamenti, immediatamente conseguenti alla variazione di funzione/ruolo/mansione del singolo soggetto, ovvero periodici aggiornamenti che coinvolgono l'intero sistema.

6. ORGANISMO DI VIGILANZA.

6.1 Identificazione e caratteristiche dell'Organismo di Vigilanza

In ottemperanza a quanto previsto all'art. 6, lettera b, del Decreto, che prevede che il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne il relativo aggiornamento sia affidato ad un organismo della società, dotato di Cdautonomi poteri di iniziativa e controllo, denominato ODV, SILAQ SERVICE ha ritenuto di nominare un ODV composto da un membro esterno nella persona dell'AvvGiuseppe Musciolà, soggetto esterno dotato di competenze necessarie allo svolgimento dell'incarico.

L'ODV è nominato dal CDA e resta in carica per la durata indicata all'atto della nomina. I suoi membri possono essere rinominati.

Ai rapporti tra l'ente e l'ODV si applicano le norme del codice civile in tema di mandato.

In considerazione della peculiarità delle proprie attribuzioni e dei propri requisiti professionali, l'ODV, nello svolgimento dei compiti che gli competono, potrà avvalersi del supporto di quelle altre funzioni aziendali di SILAQ SERVICE che di volta in volta si rendessero utili per il perseguimento del fine detto, nonché di quelle strutture aziendali specializzate che occupano specificamente parte del proprio lavoro nell'esame delle richieste di controllo e vigilanza inoltrate dall'ODV.

6.2 Funzioni e poteri dell'Organismo di Vigilanza

Da un punto di vista generale, all'ODV, spettano essenzialmente due tipi di attività, che tendono ad eliminare e/o ridurre i rischi di commissione dei reati, e più precisamente:

- a) vigilare che i Destinatari del Modello, appositamente individuati in base alle diverse fattispecie di reato, osservino le prescrizioni in esso contenute (**funzione ispettiva**);
- b) verificare i risultati raggiunti dall'applicazione del Modello in ordine alla prevenzione di reati e valutare la necessità o semplicemente l'opportunità di adeguare il Modello a norme sopravvenute ovvero alle nuove esigenze aziendali (**funzione preventiva**);
- c) In estrema sintesi, le attività di cui sopra sono finalizzate all'effettuazione, da parte dell'ODV, di una **costante vigilanza in merito al recepimento, all'attuazione e all'adeguatezza ed efficacia nel tempo del Modello, promuovendo le opportune azioni correttive.**

Qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente spetterà all'ODV adottare tutte le iniziative necessarie per correggere tale condizione:

- a) sollecitando i responsabili delle singole unità organizzative ed operative al rispetto dei modelli di comportamento;
- b) indicando direttamente quali correzioni e modifiche debbano essere apportate ai protocolli ed alle procedure aziendali;
- c) segnalando i casi di mancata attuazione del Modello ai responsabili ed agli addetti ai controlli all'interno delle singole funzioni e riportando, per i casi più gravi, direttamente alla Direzione di SILAQ SERVICE.

Qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di un adeguamento dello stesso – che, pur integralmente e correttamente attuato, si riveli non idoneo allo scopo di evitare il rischio del verificarsi di taluno dei reati previsti dal Decreto – sarà proprio l'ODV di SILAQ SERVICE a doversi attivare affinché vengano apportati, in tempi brevi, i necessari aggiornamenti.

Su di un piano più operativo, le su indicate funzioni si tradurranno nella seguenti azioni:

- a) effettuare interventi periodici (ad esempio, verifiche ispettive), sulla base di un programma annuale approvato dall'CDA, diretti a vigilare:
 - I) affinché le procedure ed i controlli contemplati dal Modello siano posti in essere e documentati in maniera conforme;
 - II) affinché i principi del Codice Etico siano rispettati;
 - III) sull'adeguatezza e sull'efficacia del Modello nella prevenzione dei reati di cui al Decreto.
- b) segnalare eventuali carenze/inadeguatezze del Modello nella prevenzione dei reati di cui al Decreto e verificare che le competenti funzioni aziendali provvedano ad implementare le misure correttive, realizzando, se necessario, manuali di controllo;
- c) suggerire procedure di verifica adeguate, ferma restando in capo all'organo dirigente di SILAQ SERVICE, ovvero agli organi sociali specificatamente deputati, la responsabilità per il controllo delle attività sociali;
- d) avviare indagini interne straordinarie laddove si sia evidenziata o sospettata la violazione del Modello ovvero la commissione dei reati;
- e) promuovere iniziative per diffondere la conoscenza e l'effettiva comprensione del Modello tra i dipendenti, i collaboratori e i terzi che comunque abbiamo rapporti con la Società, predisponendo la documentazione interna (istruzioni, chiarimenti, aggiornamenti) ovvero specifici seminari di formazione, necessari affinché il Modello possa essere compreso ed applicato;
- f) coordinarsi con i responsabili delle varie funzioni aziendali per il controllo delle attività nelle aree a rischio e confrontarsi con essi su tutte le problematiche relative all'attuazione del Modello (es. definizione c/cdasole standard per i contratti, organizzazione di corsi per il personale, ecc.). In

- particolare, l'ODV dovrà coordinarsi con l'Ufficio del personale in merito alla formazione del personale ed ai procedimenti disciplinari;
- g) coordinarsi con le altre funzioni aziendali:
- per uno scambio di informazioni finalizzato a tenere aggiornate le aree a rischio reato (ad es. le funzioni aziendali dovranno dare comunicazione per iscritto dei nuovi rapporti con la Pubblica Amministrazione non già a conoscenza dell'ODV, ovvero dell'apertura di nuovi cantieri, ecc.);
 - per tenere sotto controllo la loro evoluzione al fine di realizzare il costante monitoraggio;
 - per i diversi aspetti attinenti l'attuazione del Modello;
 - per garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace vengano intraprese tempestivamente;
- h) richiedere al Cda di mantenere il Modello aggiornato, adeguandolo alle normative sopravvenute ovvero a mutamenti organizzativi della società e/o a differenti esigenze aziendali;
- i) richiedere l'aggiornamento periodico della mappa delle attività a rischio, e verificarne l'effettivo aggiornamento attraverso il compimento di verifiche periodiche puntuali e mirate sulle attività a rischio; a tal fine all'ODV devono essere segnalate da parte dei responsabili delle diverse funzioni aziendali le eventuali situazioni che possono esporre l'Azienda al rischio di reato nell'ambito delle rispettive funzioni;
- j) raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute sul rispetto del Modello, nonché aggiornare periodicamente la lista delle informazioni che è necessario gli siano trasmesse;
- k) verificare che gli elementi previsti dalle singole Parti Speciali del presente Modello siano comunque adeguate e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto.

6.3 Prerogative e risorse dell'Organismo di Vigilanza

Per l'espletamento delle funzioni indicate, l'ODV deve avere libero accesso, senza la necessità di alcun consenso preventivo, salvi i casi in cui tale consenso preventivo sia reso necessario da leggi e regolamenti, alle persone e a tutta la documentazione aziendale, nonché la possibilità di acquisire dati ed informazioni rilevanti dai soggetti responsabili. Infine, all'ODV devono essere segnalate tutte le informazioni come di seguito specificato al punto 6.4.

L'ODV deve essere inoltre, dotato di un budget adeguato all'espletamento delle attività necessarie al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte, ecc.) e deve avere la possibilità di avvalersi di consulenti esterni, coordinandosi ed informando preventivamente le funzioni aziendali interessate.

A tal fine, l'ODV, all'inizio del proprio mandato e con cadenza annuale, presenterà all'organo dirigente una richiesta di budget di spesa annuale che SILAQ SERVICE dovrà mettere a sua disposizione; e in ogni caso

l'ODV potrà richiedere l'erogazione di somme eccedenti l'importo assegnato in ragione di eventi o circostanze straordinarie (cioè al di fuori dell'ordinario svolgimento dell'attività dell'ODV).

Infine, in relazione agli aspetti concernenti la calendarizzazione delle attività, la verbalizzazione delle riunioni, la disciplina dei flussi informativi, le modalità operative relative alla pianificazione, all'esecuzione ed ai risultati delle verifiche ispettive l'ODV dovrà emanare un regolamento a disciplina di tali aspetti, ben potendo a tal fine richiamare ed avvalersi di protocolli, procedure e modelli dei sistemi di gestione aziendale già adottati da SILAQ SERVICE.

7. FLUSSI INFORMATIVI INTERNI

7.1 *Reporting dell'Organismo di Vigilanza*

L'OdV, salve le ulteriori variazioni strutturali connesse all'evoluzione del Modello, osserverà due linee di reporting con diverso riferimento temporale:

- a) reporting periodico con cadenza semestrale al General Manager di SILAQ SERVICE;
- b) reporting periodico con cadenza annuale alla Società in ordine a quanto di seguito specificato.

Premesso che la responsabilità del Modello permane in capo all'organo dirigente di SILAQ SERVICE, l'ODV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

Più specificatamente, l'ODV nei confronti del CDA, ha la responsabilità di:

- a) comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
- b) comunicare periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli;
- c) comunicare immediatamente eventuali problematiche significative scaturite dalle attività;

L'ODV potrà essere convocato, o chiedere di essere convocato, in qualsiasi momento dai suddetti organi, per riferire sul funzionamento del Modello o su altre situazioni specifiche che si dovessero verificare volta per volta nello svolgimento della propria attività.

L'ODV potrà, inoltre, valutando le singole circostanze:

- a) comunicare i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tal caso, sarà necessario che l'ODV ottenga dai responsabili dei processi medesimi un piano delle azioni, con relativa tempistica, in ordine alle attività suscettibili di miglioramento, nonché le specifiche delle modifiche che dovrebbero essere attuate;
- b) segnalare eventuali comportamenti/azioni non in linea con il Codice Etico e con le procedure aziendali al fine di:
 - I) acquisire, sulla base di specifiche segnalazioni ricevute, o di dati oggettivi riscontrati, tutti gli elementi da eventualmente comunicare alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
 - II) evitare il ripetersi dell'accadimento, dando indicazioni per la rimozione delle carenze.

Le attività indicate al punto II dovranno, nel più breve tempo possibile, essere comunicate dall'ODV alla Direzione di SILAQ SERVICE, richiedendo anche il supporto delle strutture aziendali in grado di collaborare nell'attività di accertamento e nell'individuazione delle azioni idonee ad impedire il ripetersi di tali circostanze.

7.2 Obblighi informativi nei confronti dell'Organismo di Vigilanza

7.2.1) INFORMAZIONI PROVENIENTI DA DIPENDENTI, COLLABORATORI E TERZI IN GENERE.

Al fine di agevolare l'attività di vigilanza sull'efficacia del Modello – nonché l'accertamento delle cCdase/disfunzioni che avessero reso eventualmente possibile il verificarsi del reato – qualsiasi informazione, comunicazione e documentazione, anche se proveniente da terzi, riguardante l'attuazione del Modello va inoltrata all'ODV con le modalità stabilite dal regolamento da esso adottato o dalle procedure in questo richiamate.

Eventuali segnalazioni devono essere effettuate in forma scritta e preferibilmente NON anonima e possono avere ad oggetto ogni violazione o sospetto di violazione del Modello e del Codice Etico.

Le informative acquisite dall'ODV saranno trattate, in aderenza al Codice Etico, in modo da garantire:

- (a) il rispetto della persona, della dignità umana e della riservatezza e da evitare per i segnalanti qualsiasi forma di ritorsione, penalizzazione o discriminazione;
- (b) la tutela dei diritti di enti/società e persone in relazione alle quali sono state effettuate segnalazioni in mala fede e successivamente risultate infondate.

L'ODV valuterà le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine potrà ascoltare l'Cdatore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale Cdatonoma decisione a non procedere.

7.2.2) INFORMAZIONI OBBLIGATORIE E DELEGHE.

Sono considerate informazioni da trasmettere obbligatoriamente all'ODV quelle riguardanti:

- a) le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- b) le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al D. Lgs. n. 231/2001;

- c) provvedimenti e/o notizie, relative a SILAQ SERVICE, provenienti da organi di polizia giudiziaria o da qualsiasi altra Cdatorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
- d) le richieste di assistenza legale inoltrate dagli Amministratori, dai Dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti di cui al Decreto;
- e) le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza, da parte dell'Ufficio del personale, dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- f) le relazioni preparate da responsabili delle varie funzioni aziendali da cui emergano fatti, eventi od omissioni anche solo potenzialmente ricollegabili a fattispecie di reato previste dal Decreto;
- g) informazioni sulla evoluzione delle attività attinenti alle aree a rischio individuate dal Modello e/o sulle modifiche della organizzazione aziendale;
- h) obbligo di segnalare le operazioni atipiche, gli eventuali mutamenti di rischio, l'invio delle copie dei verbali dell'CDA.

L'ODV potrà proporre periodicamente al CDA eventuali modifiche alla casistica su indicata.

All'ODV deve essere obbligatoriamente comunicato dalla Direzione di SILAQ SERVICE il sistema delle deleghe di poteri e di firma in vigore in SILAQ SERVICE e qualsiasi modifica ad esso riferita.

8. FORMAZIONE E INFORMATIVA.

8.1 Formazione del personale

Ai fini dell'attuazione del Modello, la formazione del personale avviene secondo quanto previsto dalle specifiche procedure aziendali in essere. SILAQ SERVICE organizza periodicamente specifici eventi di formazione/informazione del personale.

8.2 Diffusione del modello e del Codice Etico al personale Dirigente e Dipendente

Un'effettiva conoscenza del presente Modello e del Codice Etico nel contesto aziendale deve essere assicurata mediante l'invio, tramite e-mail, a tutto il personale dirigente e dipendente, del relativo testo. Saranno poi organizzate specifiche attività di informazione/formazione sull'argomento, nonché fornito a tutti l'accesso ad un apposito spazio dedicato al Decreto nella rete informativa aziendale.

Saranno, inoltre, organizzate periodicamente attività di aggiornamento finalizzate all'informazione a tutto il personale circa eventuali modifiche e/o integrazioni del presente Modello.

Per tutti i nuovi assunti, oltre alla consegna del Codice Etico ed alla consegna di un'informativa contenuta nella lettera di assunzione, verranno organizzati specifici eventi informativi/formativi sull'argomento.

Ai fini di una adeguata attività di informazione/formazione, l'ODV, in stretta cooperazione con le funzioni previste dalla specifica procedura, provvederà a curare la diffusione del Modello.

8.3 Altro personale non qualificabile come dipendente

La formazione del rimanente personale non qualificabile come personale dipendente (es. Collaboratori Coordinati, Collaboratori a Progetto, Interinali, ecc.), dovrà avvenire sulla base di specifici eventi di informazione/formazione e di un'informativa per i rapporti di collaborazione di nuova costituzione.

8.4 Informativa a collaboratori esterni e terze parti

Ai fini di una adeguata attività di informazione, l'ODV, in stretta cooperazione con i responsabili delle aree interessate (settore acquisti, commerciale, gare, etc.), provvederà a definire un'informativa specifica a seconda delle terze parti interessate, nonché a curare la diffusione del contenuto del Modello e del Codice Etico adottato da SILAQ SERVICE, anche mediante la pubblicazione di entrambi sul sito internet della società.

SILAQ SERVICE, previa proposta dell'ODV, potrà, inoltre:

- a) fornire ai collaboratori adeguate informative sulle politiche e le procedure indicate nel presente Modello;
- b) dotare i collaboratori di testi contenenti le clCdasole contrattuali utilizzate al riguardo.

9. SISTEMA DISCIPLINARE

L'applicazione delle sanzioni disciplinari determinate ai sensi del Decreto prescinde dall'esito di eventuali procedimenti penali, in quanto le regole imposte dal Modello sono assunte da SILAQ SERVICE in piena Cdautonomia, indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

In particolare, si è creato un sistema disciplinare che sanziona tutte le infrazioni al Modello, dalla più grave alla più lieve, mediante un sistema di gradualità della sanzione, nel rispetto del principio di proporzionalità tra la mancanza rilevata e la sanzione comminata.

Il potere disciplinare di cui al D. Lgs. 231/2001 è esercitato su proposta dell'ODV dall'Ufficio del Personale, nel rispetto delle procedure previste dall'art. 7 dello Statuto dei Lavoratori e/o da normative speciali, dove applicabili.

9.1 Sanzioni applicabili ai dipendenti

In caso di mancato rispetto delle prescrizioni indicate nel Modello, in proporzione alla gravità delle infrazioni, verranno applicate le sanzioni qui di seguito indicate:

a) **Rimprovero verbale:**

- lieve inosservanza di quanto stabilito dalle procedure interne previste dal Modello o adozione di un comportamento negligente non conforme alle prescrizioni del Modello stesso;
- tolleranza o omessa segnalazione, da parte dei preposti, di lievi irregolarità commesse da altri appartenenti al personale.

b) **Rimprovero scritto:**

- mancanze punibili con il rimprovero verbale ma che, per conseguenze specifiche o per recidiva, abbiano una maggiore rilevanza (violazione reiterata delle procedure interne previste dal Modello o adozione ripetuta di un comportamento non conforme alle prescrizioni del Modello stesso);
- omessa segnalazione o tolleranza, da parte dei preposti, di irregolarità non gravi commesse da altri appartenenti al personale;
- ripetuta omessa segnalazione o tolleranza, da parte dei preposti, di irregolarità lievi commesse da altri appartenenti al personale.

c) **Sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni:**

- inosservanza delle procedure interne previste dal Modello o negligenze rispetto alle prescrizioni del Modello;

- omessa segnalazione o tolleranza di gravi irregolarità commesse da altri appartenenti al personale che siano tali da esporre SILAQ SERVICE ad una situazione oggettiva di pericolo o da determinare per essa riflessi negativi.

d) **Licenziamento per giustificato motivo:**

- violazione delle prescrizioni del Modello con un comportamento tale da configurare una possibile ipotesi di reato sanzionato dal D. Lgs. 231/01

e) **Licenziamento per giusta causa:**

- comportamento in palese violazione delle prescrizioni del Modello e tale da comportare la possibile applicazione a carico di SILAQ SERVICE delle sanzioni previste dal D. Lgs. 231/01, riconducibile a mancanze di gravità tale da far venire meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire comunque la prosecuzione, nemmeno provvisoria, del rapporto stesso.

9.2 *Sanzioni applicabili ai Dirigenti*

a) **Rimprovero verbale:**

- lieve inosservanza di quanto stabilito dalle procedure interne previste dal Modello o adozione di un comportamento negligente non conforme alle prescrizioni del Modello stesso;
- tolleranza o omessa segnalazione, da parte dei preposti, di lievi irregolarità commesse da altri appartenenti al personale.

b) **Rimprovero scritto:**

- mancanze punibili con il rimprovero verbale ma che, per conseguenze specifiche o per recidiva, abbiano una maggiore rilevanza (violazione reiterata delle procedure interne previste dal Modello o adozione ripetuta di un comportamento non conforme alle prescrizioni del Modello stesso);
- omessa segnalazione o tolleranza, da parte dei preposti, di irregolarità non gravi commesse da altri appartenenti al personale;
- ripetuta omessa segnalazione o tolleranza, da parte dei preposti, di irregolarità lievi commesse da altri appartenenti al personale.

c) **Licenziamento *ex art. 2118 c.c.*:**

- inosservanza delle procedure interne previste dal Modello o negligenze rispetto alle prescrizioni del Modello;
- omessa segnalazione o tolleranza di gravi irregolarità commesse da altri appartenenti al personale;

- violazione delle prescrizioni del Modello con un comportamento tale da configurare una possibile ipotesi di reato sanzionato dal D.Lgs. 231/01 e di una gravità tale da esporre SILAQ SERVICE ad una situazione oggettiva di pericolo o tale da determinare comunque riflessi negativi per la società.

d) **Licenziamento per giusta causa:**

- adozione di un comportamento palesemente in violazione alle prescrizioni del Modello e tale da determinare la possibilità di una concreta applicazione a carico di SILAQ SERVICE delle misure previste dal D. Lgs. 231/01, riconducibile a mancanze di gravità tale da far venire meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire neppure una prosecuzione provvisoria dello stesso.

9.3 Disciplina applicabile nei confronti di collaboratori esterni e partners

Al fine di una piena efficacia preventiva del Modello rispetto ai reati indicati dal D. Lgs. 231/01, sono previste misure sanzionatorie anche nei confronti di Collaboratori Esterni e Partners che pongano in essere comportamenti in contrasto con le linee di condotta indicate nel presente Modello.

Segnatamente, nei contratti stipulati tra SILAQ SERVICE e tali soggetti devono essere inserite specifiche clausole risolutive espresse che prevedano appunto la risoluzione del contratto per il caso in cui la controparte contrattuale tenga condotte in violazione delle prescrizioni di cui al presente Modello e tali da comportare il rischio di commissione di reati di cui al D. Lgs. 231/01, rimanendo salvo ed impregiudicato il diritto di SILAQ SERVICE di chiedere il risarcimento dei danni che le predette condotte cagionino a carico della società.

In considerazione di quanto sopra copia del Modello deve essere consegnata a Collaboratori Esterni e Partners.

10. VERIFICHE DELL'ODV

In relazione ai compiti di monitoraggio e di aggiornamento del Modello assegnati all'ODV dall'art. 6, comma 1 lett. b), D. Lgs. 231/2001, il Modello sarà soggetto a tre tipi di verifiche:

- I) Verifiche Ispettive sul rispetto delle misure di prevenzione previste dalle singole Parti Speciali in relazione alle aree ed al tipo di rischio reato preso in considerazione;
- II) verifiche periodiche sull'effettivo funzionamento del Modello e delle procedure implementative del medesimo con le modalità stabilite dall'ODV;
- III) riesame annuale di tutte le segnalazioni ricevute nel corso dell'anno, le azioni intraprese in proposito dall'ODV e dagli altri soggetti interessati, gli eventi e gli episodi considerati maggiormente rischiosi, nonché l'effettività della conoscenza tra tutti Destinatari del contenuto del Modello, delle ipotesi di reato previste dal Decreto e del Codice Etico.

L'ODV procede alle Verifiche Ispettive in modo pianificato su tutte le aree rischio reato, attraverso sopralluoghi e attività di analisi di singole procedure gestionali o di intere aree aziendali.

La frequenza delle Verifiche Ispettive può variare in funzione della complessità dell'area/procedura da verificare o di eventuali criticità emerse nel corso di verifiche precedenti.

A fine anno è responsabilità dell'ODV redigere il Programma di Verifiche Ispettive (PVI) per l'anno successivo da sottoporre all'approvazione del CDA. Gli interventi programmati potranno comunque essere integrati da verifiche addizionali che si rendano necessarie ed opportune, i cui estremi dovranno essere riportati sul PVI.

E' compito dell'ODV:

- concordare, ove necessario, le date di effettuazione delle singole verifiche con i responsabili delle aree interessate;
- predisporre il Rapporto di Verifica Ispettiva da cui risultino, oltre alle annotazioni eventualmente richieste dalle previsioni delle singole Parti Speciali in considerazione dell'area di rischio reato interessata, riscontri oggettivi circa 1) le modalità di circolazione delle informazioni; 2) la completezza e la corretta utilizzazione e conservazione dei documenti; 3) il corretto svolgimento delle attività aziendali; 4) ogni utile annotazione per una valutazione globale della verifica e per la definizione delle azioni correttive che si rendessero necessarie.

La verifica può essere preceduta da una riunione iniziale tra l'ODV ed il Responsabile dell'area interessata, nella quale discutere i contenuti, i tempi e le modalità della verifica.

Dei risultati di questa attività di verifica dovrà dare conto, seppure sommariamente, la relazione annualmente predisposta dall'ODV per il CDA di SILAQ SERVICE.

11. MODELLO E CODICE ETICO

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico.

Il Codice Etico rappresenta uno strumento adottato dal CDA di SILAQ SERVICE e suscettibile di applicazione sul piano generale allo scopo di esprimere dei principi di "deontologia aziendale" che SILAQ SERVICE riconosce come propri e sui quali richiama l'osservanza da parte di tutti i dipendenti, i dirigenti, gli amministratori, i collaboratori esterni e i partner di affari.

Il Modello risponde a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati.

I principi contenuti nel Codice Etico, afferenti ai temi trattati nella Parte Generale e nelle Parti Speciali del Modello, costituiscono le regole comportamentali di base per il legittimo esercizio delle attività aziendali.

Il Codice Etico è allegato al presente Modello di cui costituisce parte integrante.

12. PROCEDURA PER LA GESTIONE DI SEGNALAZIONI DI ILLECITI E MISURE A TUTELA DEL SEGNALANTE (C.D. WHISTLEBLOWER)

Sommario

Premessa

1. Soggetti, oggetto e destinatari della segnalazione
 2. Modalità di segnalazione
 3. Verifica, accertamento ed esiti delle segnalazioni
 4. Tutela del segnalante
 5. Segnalazione di comportamenti discriminatori
 6. Iniziative di sensibilizzazione
 7. Modifiche delle misure di prevenzione dei rischi
 8. Revisione periodica della presente procedura
- Allegato 1 - Modulo per la Segnalazione di Condotte Illecite
Allegato 2 - Appendice normativa

Premessa

La legge n. 179/2017, promulgata in data 30.11.2017, ha introdotto (sulla scia della legge 6 novembre 2012, n. 190 e s.m.i. - normativa in materia di prevenzione della corruzione e dell'illegalità nella pubblica amministrazione) anche per i dipendenti del settore privato un nuovo strumento per facilitare la

segnalazione di comportamenti che potrebbero costituire illeciti, in particolare di natura corruttiva, stabilendo che chi, in buona fede, denuncia all' Cdatorità giudiziaria o alla Corte dei conti o all' Cdatorità nazionale anticorruzione (ANAC) o riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto a una misura discriminatoria, diretta o indiretta, avente effetto sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia.

Tale strumento è stato originariamente previsto dall'art. 54 bis del d.lgs. 165/2001, introdotto dalla legge n. 190/2012 e in seguito modificato dal d. l. 24 giugno 2014, n. 90, convertito in legge 11 agosto 2014, n. 114, che titola "Tutela del dipendente pubblico che segnala illeciti" (c.d. whistleblower).

La legge 179/2017 sul whistleblowing ha modificato l'articolo 54 bis del d.lgs. 165/2001: ora è previsto che il pubblico dipendente, al fine di salvaguardare l'integrità ed il buon funzionamento della pubblica amministrazione, può segnalare al "Responsabile delle prevenzione delle corruzione e della trasparenza" (Rpct) - sostituendo così il riferimento al "superiore gerarchico" - ovvero all' Cdatorità nazionale anticorruzione (Anac) o direttamente all' Cdatorità giudiziaria o contabile, le condotte illecite di cui sia venuto a conoscenza, prescrivendo che in alcun modo il medesimo possa essere sanzionato, trasferito, demansionato, licenziato o sottoposto ad altra misura organizzativa tale da produrre ripercussioni negative dirette o indirette sulle sue condizioni di lavoro.

Essenziale è garantire la riservatezza dei dati del segnalante, che può venire meno solo in occasione dei procedimenti disciplinari laddove la rivelazione dell'identità del segnalante diviene indispensabile per consentire la difesa dell'incolpato.

Indicazioni utili per l'attuazione di questa disposizione di legge si rinvencono nel Piano Nazionale Anticorruzione adottato con deliberazione n. 72 dell'11.09.2013 dalla Commissione Indipendente per la Valutazione, la Trasparenza e l'Integrità delle Amministrazioni Pubbliche (C.I.V.I.T.) - ora Cdatorità Nazionale Anticorruzione (A.N.A.C.) - e nella Determinazione A.N.A.C. n. 6 del 28 aprile 2015, "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)".

Come detto sopra, la normativa è nata per il settore pubblico ed è stata estesa al settore privato con la legge n. 179/2017. Con la nuova normativa, pertanto, anche il whistleblower occupato in un'azienda privata deve poter fare affidamento sulla presenza di procedure dirette a preservare lo stretto riserbo sull'identità della propria persona e sul contenuto delle segnalazioni presentate. La legge n. 179/2017 ha pertanto rivisto la formulazione dell'art. 6 del d.lgs. 231/01, stabilendo che i Modelli organizzativi debbano prevedere uno o più canali che consentano ai soggetti apicali e ai dipendenti di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del d.lgs. 231/01 e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente

La presente procedura costituisce parte integrante del Modello di Organizzazione e Gestione ex d.lgs. 231/01 di SILAQ SERVICE.

Fatti salvi gli obblighi di legge, tutti coloro che ricevano una segnalazione o vengano a conoscenza della stessa o siano coinvolti a qualsiasi titolo nel processo di gestione della stessa devono osservare la massima

riservatezza al fine di tutelare da un lato l'anonimato del segnalante, affinché non subisca ritorsioni, e dall'altra la reputazione dei soggetti segnalati, poiché quanto riportato potrebbe non corrispondere al vero. Qualora la segnalazione non sia stata fatta in buona fede, il segnalante è sottoposto a procedimento disciplinare, al termine del quale potranno essere inflitte le misure sanzionatorie in conformità a quanto stabilito dai contratti collettivi.

1. Soggetti, oggetto e destinatari della segnalazione

A) I soggetti che sono tutelati ai sensi della presente disciplina sono i dipendenti di SILAQ SERVICE sia con contratto di lavoro a tempo indeterminato sia con contratto di lavoro a tempo determinato. A questi si aggiungono i collaboratori di SILAQ SERVICE qualunque sia il rapporto di lavoro intercorrente: Cdatonomo, di consulenza, di collaborazione.

B) L'oggetto della segnalazione è ampio e comprende azioni od omissioni che:

- costituiscono reato, per esempio, contro la Pubblica Amministrazione come da Libro II - Titolo II del Codice penale (a mero titolo esemplificativo: peculato – art. 314, malversazione – art. 316 bis, indebita percezione di erogazioni – art. 316 ter, concussione – art. 317, corruzione – art. 318, induzione indebita a dare o promettere utilità – art. 319 quater, abuso d'ufficio – art. 323, rivelazione e utilizzazione di segreti d'ufficio – art. 326, turbata libertà degli incanti – art. 353; turbata libertà del procedimento di scelta del contraente – art. 353 bis, ecc.), contro la persona come da Libro II – Titolo XII del Codice penale (a mero titolo esemplificativo: violenza – art. 610, minaccia – art. 612, ecc), contro il patrimonio (furto – art. 624, truffa – art. 640).;
- possono comportare danni patrimoniali a SILAQ SERVICE o alla collettività;
- costituiscono violazioni alle disposizioni del Codice Etico SILAQ SERVICE volte a evitare la commissione di reati. Infine, va considerato che, ai fini delle segnalazioni, il dipendente deve prendere in considerazione non solo quelle situazioni che configurano reati di corruzione (art. 318, 319 e 319 ter, 319 quater del Codice penale), ma anche quelle 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* (come precisato dalla Circolare 1/2013 emanata dal Dipartimento della Funzione pubblica). Non sono prese in considerazione, ai fini della normativa in argomento, le segnalazioni riguardanti situazioni di carattere personale aventi a oggetto rivendicazioni o rimostranze relative ai rapporti con i superiori gerarchici o i colleghi o relative all'esecuzione della propria prestazione lavorativa.

C) Il soggetto destinatario della segnalazione è il Team Whistleblowing, composto dal membro dell'Organismo di Vigilanza (Avv. Giuseppe Musciolà) nominato dalla Società ex d.lgs. 231/01 (di seguito OdV). Il segnalante può anche destinare la propria segnalazione a uno solo dei soggetti sopra citati, ma deve precisarsi che in tal caso il soggetto che ha ricevuto la segnalazione deve dare notizia all'altro

membro delle segnalazioni singolarmente ricevute, salvo che oggetto della segnalazione non siano comportamenti del suddetto.

2. Modalità di segnalazione

Le segnalazioni devono essere circostanziate, avere a oggetto fatti conosciuti e riscontrati direttamente dal segnalante – e non riferiti da altri – e, se possibile, individuare con certezza l'Autore della condotta illecita. Le segnalazioni possono essere inoltrate con qualsiasi modalità; tuttavia, al fine di perseguire la miglior tutela della riservatezza del segnalante, si suggeriscono le seguenti:

- a) mediante invio, dalla propria casella di posta elettronica aziendale o da quella privata, all'indirizzo di posta elettronica appositamente attivato dalla Società (*odv@SilaqService.it*), accessibile esclusivamente ai componenti del Team Whistleblowing sopra citato;
- b) mediante il servizio postale, con busta chiusa e contrassegnata come "RISERVATA", che può essere indirizzata al Team Whistleblowing oppure al Responsabile Prevenzione Corruzione oppure all'Organismo di Vigilanza, presso SILAQ SERVICE S.r.l., Piazza Castello n. 26, 20121 Milano, con le seguenti ulteriori opzioni alternative:

- con i dati identificativi del segnalante "in chiaro" e copia del documento d'identità, siglato con firma Cdatografa;
- con un'altra busta chiusa, contenuta nella busta, contenente le generalità del segnalante e copia del documento d'identità dello stesso, siglato con firma autografa;

- c) con segnalazione verbale al componente l'OdV. I destinatari della segnalazione dovranno redigere apposito verbale alla presenza del segnalante e di almeno un altro componente del Team Whistleblowing.

I soggetti che ricevono le segnalazioni devono mantenere riservata l'identità del soggetto segnalante.

SILAQ SERVICE mette a disposizione di tutti i soggetti legittimati a inoltrare le segnalazioni un apposito modulo pubblicato sulla rete Intranet (Allegato 1). La segnalazione potrà essere presentata anche con dichiarazione diversa da quella prevista nel predetto modulo.

Per quanto riguarda invece gli adempimenti relativi alla denuncia alla competente Procura della Repubblica presso la Corte dei Conti di fatti che possano dar luogo a responsabilità per danni cagionati alla finanza pubblica, si fa rinvio alle indicazioni operative riportate nella nota interpretativa del Procuratore Generale presso la Corte dei Conti del 2 agosto 2007 (Prot. N. PG/9434/2007/P).

In entrambi i casi sopra citati troveranno attuazione, a favore del segnalante, le disposizioni previste dalla presente disciplina a tutela dello stesso.

2. Verifica, accertamento ed esiti delle segnalazioni

Il Team Whistleblowing, ricevuta la segnalazione, procede a una prima verifica del contenuto dei fatti segnalati, da concludersi nel più breve tempo possibile e in ogni caso non oltre trenta giorni. Nel caso la

segnalazione appaia a prima vista non palesemente infondata, i fatti segnalati saranno comunicati senza indugio all'CDCA mantenendo riservate le generalità del segnalante.

Il Team Whistleblowing ai fini della verifica di cui sopra potrà:

- interloquire, anche direttamente, con il segnalante avendo cura di adottare tutte le cautele per garantire la massima riservatezza;
- trasmettere la segnalazione, dopo averla resa completamente anonima e/o riprodotta per renderla non riconoscibile, ad altri soggetti per acquisire ulteriori informazioni e osservazioni. Tali soggetti dovranno formulare le proprie valutazioni entro e non oltre quindici giorni dalla ricezione della richiesta.

Qualora, all'esito degli accertamenti eseguiti, la segnalazione risulti: infondata o non sufficientemente circostanziata o non pertinente, il Team Whistleblowing procederà all'archiviazione, informandone l'CDCA e mantenendo riservate le generalità dei soggetti segnalati e dei segnalanti. Nel caso la segnalazione risulti fondata, il Team Whistleblowing provvederà a comunicare l'esito della propria valutazione e/o verifica all'CDCA, mantenendo riservate le generalità del segnalante. Il Team Whistleblowing trasmetterà periodicamente all'CDCA un report contenente l'elenco delle segnalazioni ricevute nel periodo e l'esito delle attività di verifica svolte, mantenendo riservate le generalità dei segnalati e dei segnalanti.

Nel caso in cui i soggetti costituenti il Team Whistleblowing fossero in disaccordo circa la valutazione della segnalazione, potranno formulare separatamente le proprie conclusioni all'CDCA, nel rispetto e a tutela delle rispettive prerogative di autonomia.

L'CDCA informerà il Team Whistleblowing degli esiti della propria valutazione in merito alle segnalazioni ricevute.

Qualora in relazione alla natura della violazione sussistano le condizioni di legge, l'CDCA presenterà denuncia all'Autorità Giudiziaria competente, informandone il Team Whistleblowing.

Il Team Whistleblowing informerà il segnalante dell'esito della segnalazione entro 15 giorni dal ricevimento delle relative comunicazioni da parte del CDA.

4. Tutela del segnalante

L'identità del segnalante è tutelata in tutte le fasi della procedura descritta ai paragrafi che precedono. Pertanto, la stessa non può essere rivelata senza il consenso espresso del segnalante; tale tutela vale anche nei confronti degli organi di vertice della Società, che non possono disporre indagini o chiedere informazioni al fine di risalire all'identità del segnalante.

L'obbligo di mantenere la massima riservatezza sull'identità del segnalante e di non svolgere indagini o chiedere informazioni di cui al comma precedente riguarda tutti coloro che, a qualunque titolo, vengano a conoscenza della stessa o siano coinvolte nel procedimento di accertamento della segnalazione e potrà essere ribadito anche tramite richiesta di sottoscrizione di un formale impegno in tal senso.

In caso di attivazione di procedimento disciplinare a seguito dei fatti oggetto della segnalazione, l'identità del segnalante potrà essere rivelata qualora la contestazione dell'addebito disciplinare risulti fondata, in

tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato, sempre che tale circostanza venga da quest'ultimo dedotta e comprovata in sede di Cdadizione o mediante la presentazione di memorie difensive.

La norma citata (art. 54 bis D. Lgs. n. 165/2001, come modificata dalla legge n. 179/2017) prevede altresì al comma 1 che i dipendenti, che denunciano all' Cdatorità giudiziaria, alla Corte dei Conti, ad ANAC o riferiscano al proprio superiore gerarchico di condotte illecite conosciute in occasione del rapporto di lavoro, non possano essere sanzionati, licenziati o sottoposti a misure discriminatorie, dirette o indirette, aventi effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia.

Il superiore gerarchico, che riceva una segnalazione da un proprio collaboratore, deve informare il Team Whistleblowing.

La violazione della tutela della riservatezza del segnalante, fatti salvi i casi in cui sia ammessa la rivelazione dell'identità come sopra evidenziato, è fonte di responsabilità disciplinare per inosservanza di disposizioni di servizio.

Infine, sempre ai sensi dell'art. 54 bis del D. Lgs. 165/2001, la denuncia di condotte illecite è sottratta all'accesso agli atti di cui all'art. 22 e seguenti della legge 241/1990 e s.m.i.

Non è dovuta alcuna tutela nel caso in cui il segnalante incorra, con propria denuncia, in responsabilità penale a titolo di calunnia (art. 368 c.p.) o diffamazione (art. 595 c.p.).

5. Segnalazione di comportamenti discriminatori

SILAQ SERVICE tutela il segnalante da qualsiasi forma di ritorsione o discriminazione, diretta o indiretta (quali, ad esempio, trasferimenti, sanzioni disciplinari, mobbing, licenziamento ecc.), applicando nei confronti degli Cdatori della stessa, le sanzioni disciplinari previste nel CCNL di riferimento e fatte salve le ulteriori forme di responsabilità previste dall'ordinamento vigente a carico di questi (responsabilità disciplinare, civile, penale, amministrativa-contabile).

Il dipendente che ritiene di aver subito una discriminazione per il fatto di aver effettuato una segnalazione di illecito deve dare notizia circostanziata della discriminazione al Responsabile della Funzione Risorse Umane e informare il Team Whistleblowing.

Il Team Whistleblowing valuta la sussistenza degli elementi per effettuare la segnalazione di quanto accaduto al CDA, affinché quest'ultimo adotti tutte le iniziative necessarie e opportune.

L'ODV, nella relazione annuale prescritta dall'art.1, comma 14 della legge 190/2012, darà conto dello stato di attuazione dell'istituto del whistleblowing e degli esiti della sua applicazione da parte del personale.

6. Iniziative di sensibilizzazione

Il Team Whistleblowing intraprende iniziative di comunicazione e sensibilizzazione della procedura mediante divulgazione sul portale intranet e tramite iniziative di formazione a tutto il personale sulle finalità

dell'istituto e sul suo utilizzo, sui relativi diritti e obblighi, sulle conseguenze degli abusi nel suo utilizzo, nonché sui risultati che l'attuazione della norma ha prodotto.

7. Modifiche delle misure di prevenzione dei rischi

Qualora, a seguito delle segnalazioni, emergano elementi oggettivi idonei a denotare eventuali criticità sull'efficacia del Modello ex d.lgs. 231/01 vigente, il Team Whistleblowing predisponde la modifica dello stesso, con adozione di misure preventive ulteriori, rispetto a quelle già adottate e inserite nel Modello.

Qualora, a seguito delle segnalazioni e delle comunicazioni nei confronti degli organi sociali, emergano elementi oggettivi idonei a rivelare eventuali carenze dei sistemi di controllo interno, gli organi sociali provvedono tempestivamente al loro adeguamento.

8. Revisione periodica della presente procedura

La presente procedura può essere oggetto di revisione periodica, a seguito di confronto con uffici o dipendenti della Società e con le organizzazioni sindacali oppure a seguito di modifiche alla normativa di riferimento.

Allegato 1 - Modulo per la Segnalazione di Condotte Illecite ex L. 179/2017

La scelta di compilare tutti o alcuni dei campi del presente modulo è **FACOLTATIVA** (fatta eccezione per l'identità del segnalante, sempre obbligatoria).

NOME E COGNOME DEL SEGNALANTE: _____

QUALIFICA O POSIZIONE PROFESSIONALE: _____

SEDE DI SERVIZIO: _____

DATA/PERIODO IN CUI SI È VERIFICATO IL FATTO: (gg/mm/aaaa) _____

LUOGO FISICO IN CUI SI È VERIFICATO IL FATTO:

- UFFICIO (indicare denominazione e ubicazione della struttura):

- ALL'ESTERNO DELL'UFFICIO (indicare luogo ed indirizzo):

NATURA DELLE AZIONI/OMISSIONI COMMESSE O TENTATE:

- penalmente rilevanti;
- poste in essere in violazione del Codice Etico aziendale o di altre disposizioni sanzionabili in via disciplinare;
- suscettibili di arrecare un pregiudizio patrimoniale all'Azienda;
- suscettibili di arrecare un pregiudizio alla immagine dell'Azienda;
- altro(specificare): _____

DESCRIZIONE DEL FATTO (CONDOTTA ED EVENTO):

CDATORE/I DEL FATTO:

ALTRI EVENTUALI SOGGETTI A CONOSCENZA DEL FATTO E/O IN GRADO DI RIFERIRE SUL MEDESIMO:

EVENTUALI ALLEGATI A SOSTEGNO DELLA SEGNALAZIONE (allegare documento di identità del segnalante o altra documentazione ritenuta rilevante ai fini della segnalazione):

Il segnalante è consapevole delle responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci e/o formazione o uso di atti falsi, anche ai sensi e per gli effetti dell'art. 76 del d.P.R. 445/2000.

Luogo e data

Firma

INFORMATIVA SULLA PRIVACY: Ai sensi del GDPR privacy (di seguito “Codice Privacy”) si informa che tutti i dati forniti saranno trattati esclusivamente al fine di consentire verifiche sulle segnalazioni di irregolarità di cui al presente modulo, come previsto nella Procedura per la gestione di segnalazioni di illeciti e misure a tutela del segnalante (cd. “whistleblower”) adottata al fine di regolamentarne la gestione delle segnalazioni stesse. Il trattamento è effettuato su supporti cartacei o con l’Cdasilio di mezzi elettronici o comunque Cdatomatizzati. Il trattamento dei dati sarà effettuato con logiche di organizzazione previste dalla Procedura sopra indicata, correlate alle finalità di cui alla presente informativa, comunque, in modo da garantire la sicurezza e la riservatezza dei dati. I dati conferiti saranno trattati e conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati. Titolare del trattamento dei dati è SILAQ SERVICE S.r.l., Via Italia n. 50, 20900 Monza, nella persona del suo legale rappresentante *pro tempore*. Come indicato nella Procedura, la responsabilità della gestione della segnalazione è demandata al Team Whistleblowing, composto dall’Organismo di Vigilanza della Società ex D.Lgs. 231/01 (OdV). I dati connessi alla segnalazione saranno comunicati all’Cdatorità Giudiziaria competente qualora la società, in presenza dei presupposti di legge, presenti apposita denuncia.

Il Segnalante potrà esercitare, in qualunque momento, i diritti sanciti dall’art. 7 e 8 del D.Lgs. 196/2003, fra cui quello di accedere ai dati personali che lo riguardano, ottenerne l’aggiornamento, la rettificazione, l’integrazione oppure la cancellazione o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi da evidenziare nella richiesta, fatta salvo diversa disposizione di legge, contattando il Titolare del trattamento mediante lettera raccomandata con ricevuta di ritorno, indirizzata a: SILAQ SERVICE S.r.l., Organismo di Vigilanza ex D. Lgs. 231/01 - con sede in 20121 Milano, Piazza Castello n. 26.

Allegato 2**Appendice normativa:**

Legge 30 novembre 2017, n. 179: Disposizioni per la tutela degli Cdatori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato. (17G00193). Note: Entrata in vigore del provvedimento: 29/12/2017

La **Legge 190/2012** non contiene una definizione univoca di “*corruzione*”. Il concetto è tuttavia desumibile da quanto espressamente indicato dal Piano Nazionale Anticorruzione (e ulteriormente confermato nell’aggiornamento del PNA dell’ottobre 2015 a pag. 7) e dalla Circolare n. 1 del 25.01.2013 del Dipartimento della Funzione Pubblica, secondo cui la corruzione va intesa in senso lato, come comprensiva “*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. Le situazioni rilevanti sono quindi evidentemente più ampie della fattispecie penalistica disciplinata negli artt. 318, 319 e 319-ter del Codice Penale e sono tali da comprendere non solo l’intera gamma dei delitti contro la pubblica amministrazione disciplinati nel titolo II, Capo I del Codice Penale, ma anche le situazioni in cui – a prescindere dalla rilevanza penale – venga in evidenza un malfunzionamento dell’amministrazione a c.d. uso ai fini privati delle funzioni attribuite*”.

D. Lgs. 30.03.2001, n. 165 Art. 54-bis. Tutela del dipendente pubblico che segnala illeciti (*articolo introdotto dall’art. 1, comma 51, legge n. 190 del 2012*) 1. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell’articolo 2043 del codice civile, il pubblico dipendente che denuncia all’Cdatorità giudiziaria o alla Corte dei conti o all’Cdatorità nazionale anticorruzione (ANAC), ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia. (*comma così modificato dall’art. 31, comma 1, legge n. 114 del 2014*). 2. Nell’ambito del procedimento disciplinare, l’identità del segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell’addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione, l’identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell’incolpato. 3. L’adozione di misure discriminatorie è segnalata al Dipartimento della funzione pubblica, per i provvedimenti di competenza, dall’interessato o dalle organizzazioni sindacali maggiormente rappresentative nell’amministrazione nella quale le stesse sono state poste in essere. 4. La denuncia è sottratta all’accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n.241, e successive modificazioni».

Codice Penale: Titolo II - Dei delitti contro la Pubblica Amministrazione Capo I - Dei delitti dei pubblici ufficiali contro la Pubblica Amministrazione

Art. 314. Peculato.

Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa mobile altrui, se ne appropria, è punito con la reclusione da quattro a dieci anni. Si applica 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, dopo l'uso momentaneo, è stata immediatamente restituita.

Art. 316. Peculato mediante profitto dell'errore altrui

Il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni.

Art. 316 bis. Malversazione a danno dello Stato.

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

Art. 316 ter. Indebita percezione di erogazioni a danno dello Stato.

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

Art. 317. Concussione.

Il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei a dodici anni.

Art. 318. Corruzione per l'esercizio della funzione.

Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da uno a cinque anni.

Art. 319. Corruzione per un atto contrario ai doveri d'ufficio.

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

Art. 319-quater. Induzione indebita a dare o promettere utilità.

Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da tre a otto anni. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni.

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

Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. In ogni caso, le pene sono ridotte in misura non superiore a un terzo.

Art. 322. Istigazione alla corruzione.

Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo. Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.

La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri. La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

Art. 323. Abuso di ufficio.

Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da uno a quattro anni. La pena è Cdamentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità.

Art. 326. Rivelazione ed utilizzazione di segreti di ufficio.

Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie d'ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni. Se l'agevolazione è soltanto colposa, si applica la reclusione fino a un anno. Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, per procurare a sé o ad altri un indebito profitto patrimoniale, si avvale illegittimamente di notizie d'ufficio, le quali debbano rimanere segrete, è punito con la reclusione da due a cinque anni. Se il fatto è commesso al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto, si applica la pena della reclusione fino a due anni.

Art. 331. Interruzione di un servizio pubblico o di pubblica necessità

Chi, esercitando imprese di servizi pubblici [c.p. 358] o di pubblica necessità [c.p. 359], interrompe il servizio, ovvero sospende il lavoro nei suoi stabilimenti, uffici o aziende, in modo da turbare la regolarità del servizio, è punito con la reclusione da sei mesi a un anno e con la multa non inferiore a euro 516 I capi, promotori od organizzatori sono puniti con la reclusione da tre a sette anni e con la multa non inferiore a euro 3.098 [c.p. 29, 31, 32].

Art. 346 bis. Traffico di influenze illecite

Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 319 e 319-ter, sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente fa dare o promettere, a sè o ad altri, denaro o altro vantaggio patrimoniale, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio ovvero per remunerarlo, in relazione al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio, è punito con la reclusione da uno a tre anni.

La stessa pena si applica a chi indebitamente dà o promette denaro o altro vantaggio patrimoniale. La pena è Cdamentata se il soggetto che indebitamente fa dare o promettere, a sè o ad altri, denaro o altro vantaggio patrimoniale riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio. Le pene sono altresì Cdamentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie. Se i fatti sono di particolare tenuità, la pena è diminuita.

Art. 353. Turbata libertà degli incanti.

Chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi frCdadolenti, impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni, ovvero ne allontana gli offerenti, è punito con la reclusione da sei mesi a cinque anni (1) e con la multa da euro 103 a euro 1.032.

Se il colpevole è persona preposta dalla legge o dall'Cdatorità agli incanti o alle licitazioni suddette, la reclusione è da uno a cinque anni e la multa da euro 516 a euro 2.065. Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati, dirette da un pubblico ufficiale o da persona legalmente Cdatorizzata; ma sono ridotte alla metà.

Art. 353 bis Turbata libertà del procedimento di scelta del contraente.

Salvo che il fatto costituisca più grave reato, chiunque con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi frCdadolenti, turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.

Codice Civile:

Art. 2635. Corruzione tra privati. Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni. Si applica la pena della reclusione

fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma. Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste. Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni. Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

Titolo III - Dei delitti contro l'Amministrazione della giustizia Capo I - Dei delitti contro l'attività giudiziaria

Art. 368. Calunnia. Chiunque, con denuncia, querela, richiesta o istanza, anche se anonima o sotto falso nome, diretta all' Cdatorità giudiziaria o ad un'altra Cdatorità che a quella abbia obbligo di riferirne o alla Corte penale internazionale, incolpa di un reato taluno che egli sa innocente, ovvero simula a carico di lui le tracce di un reato, è punito con la reclusione da due a sei anni.

La pena è Cdamentata se s'incolpa taluno di un reato pel quale la legge stabilisce la pena della reclusione superiore nel massimo a dieci anni, o un'altra pena più grave. La reclusione è da quattro a dodici anni, se dal fatto deriva una condanna alla reclusione superiore a cinque anni; è da sei a venti anni, se dal fatto deriva una condanna all'ergastolo; [...].

Titolo XII - Dei delitti contro la persona Capo I - Dei delitti contro la vita e l'incolumità individuale

Art. 595. Diffamazione. Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a euro 2.065. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza o ad una Cdatorità costituita in collegio, le pene sono Cdamentate.

Sezione III - Dei delitti contro la libertà morale

Art. 610. Violenza privata. Chiunque, con violenza o minaccia, costringe altri a fare, tollerare, od omettere qualche cosa è punito con la reclusione fino a quattro anni. La pena è Cdamentata se concorrono le condizioni prevedute dall'articolo 339.

Art. 612. Minaccia. Chiunque minaccia ad altri un ingiusto danno è punito, a querela della persona offesa [120-126; c.p.p. 336], con la multa fino a euro 1.032. Se la minaccia è grave o è fatta in uno dei modi indicati nell'articolo 339, la pena è della reclusione fino a un anno e si procede d'ufficio.

Titolo XIII - Dei delitti contro il patrimonio Capo I - Dei delitti contro il patrimonio mediante violenza alle cose o alle persone

Art. 624. Furto. Chiunque s'impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 154

a euro 516. Agli effetti della legge penale, si considera cosa mobile anche l'energia elettrica e ogni altra energia che abbia un valore economico. Il delitto è punibile a querela della persona offesa, salvo che ricorra una o più delle circostanze di cui agli articoli 61, numero 7), e 625.

Capo II - Dei delitti contro il patrimonio mediante frode

Art. 640. Truffa. Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell' autorità; 2 bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.

Codice di Procedura Penale:

LIBRO QUINTO - INDAGINI PRELIMINARI E UDIENZA PRELIMINARE TITOLO II - Notizia di reato

Art. 331. Denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio. 1. Salvo quanto stabilito dall'articolo 347, i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a cCdas delle loro funzioni o del loro servizio, hanno notizia di reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito. 2. La denuncia è presentata o trasmessa senza ritardo al pubblico ministero o a un ufficiale di polizia giudiziaria. 3. Quando più persone sono obbligate alla denuncia per il medesimo fatto, esse possono anche redigere e sottoscrivere un unico atto. 4. Se, nel corso di un procedimento civile o amministrativo, emerge un fatto nel quale si può configurare un reato perseguibile di ufficio, l' autorità che procede redige e trasmette senza ritardo la denuncia al pubblico ministero.

PARTE SPECIALE “A”

REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)

Gli artt. 24 e 25 D. Lgs. 231/01 individuano un gruppo di reati che possono essere commessi nell'ambito dei rapporti che la società intrattiene con la Pubblica Amministrazione.

E' opportuno, anzitutto, che il Modello li indichi e li descriva a tutti i suoi destinatari.

1.1 Premessa: i Concetti di Pubblico Ufficiale e di Incaricato di Pubblico Servizio

Buona parte dei reati contemplati dagli artt. 24 e 25 del D. Lgs. 231/01 integrano delle fattispecie c.d. proprie, in quanto possono essere commessi unicamente da soggetti dotati della qualifica di “pubblico ufficiale” e di “incaricato di pubblico servizio”.

Agli effetti della legge penale è pubblico ufficiale (art. 357 c.p.) chi esercita una pubblica funzione legislativa, amministrativa o giudiziaria formando o concorrendo a formare la volontà sovrana dello Stato o do altro Ente pubblico presso il quale è chiamato ad esplicare mansioni deliberative, consultive o esecutive.

I *‘pubblici poteri’* qui in rilievo, dunque, sono: il *potere legislativo*, quello *giudiziario* e, da ultimo, quelli riconducibili alla *‘pubblica funzione amministrativa’*.

Il *potere legislativo* trova la sua esplicazione nell'attività normativa vera e propria ovvero in tutte quelle accessorie e/o preparatorie di quest'ultima. E' un PU, in quanto svolge la *‘pubblica funzione legislativa’*, dunque, chiunque, al livello nazionale e comunitario, partecipi all'esplicazione di tale potere. I soggetti pubblici a cui, normalmente, può ricondursi l'esercizio di tale tipo di funzione sono: il Parlamento, il Governo (limitatamente alle attività legislative di sua competenza: es., decreti legge e decreti delegati), le Regioni e le Province (queste ultime per quanto attinenti alla loro attività normativa); le Istituzioni dell'Unione Europea aventi competenze legislative rilevanti nell'ambito dell'ordinamento nazionale.

Il *potere giudiziario* trova la sua esplicazione nell'attività dello *ius dicere*, inteso in senso lato. Si ritiene, dunque, che sia un PU, in quanto svolge la *‘pubblica funzione giudiziaria’* non solo chiunque, al livello nazionale e comunitario, compia attività diretta esplicazione di tale potere, ma altresì tutta l'attività afferente l'amministrazione della giustizia, collegata ed accessoria alla prima. Svolgono tale tipo di funzione, pertanto, tutti coloro che, al livello nazionale e comunitario, partecipano sia alla vera e propria attività dello *ius dicere*, sia a quella amministrativa collegata allo stesso, ovverosia i magistrati (ivi compresi i Pubblici Ministeri), i cancellieri, i segretari, i membri della Corte di Giustizia e della Corte dei Conti Comunitarie, i funzionari e gli addetti a svolgere l'attività amministrativa collegata allo *ius dicere* della Corte di Giustizia e della Corte dei Conti Comunitarie, etc.

I *poteri* riconducibili alla *‘pubblica funzione amministrativa’*, da ultimo, sono il *potere deliberativo*, il *potere Cdatoritativo* ed il *potere certificativo* della Pubblica Amministrazione. Questi poteri, in nessun modo connessi a

particolari qualifiche soggettive e/o mansioni dei soggetti agenti, possono essere qualificati nei termini che seguono:

- il *potere deliberativo* della PA è quello relativo alla “*formazione e manifestazione della volontà della Pubblica Amministrazione*”. Questa formula è letta, in senso assai lato e, pertanto, comprensiva di qualsiasi attività che concorra in qualunque modo ad estrinsecare il potere deliberativo della Pubblica Amministrazione; in tale prospettiva, sono stati qualificati come ‘*pubblici ufficiali*’, non solo le persone istituzionalmente preposte ad esplicare tale potere ovvero i soggetti che svolgono le attività istruttorie o preparative all’*iter* deliberativo della Pubblica Amministrazione, ma anche i loro collaboratori, saltuari ed occasionali;
- il *potere Cdatoritativo* della PA, diversamente, si concretizza in tutte quelle attività che permettono alla Pubblica Amministrazione di realizzare i suoi fini mediante veri e propri comandi. Questo ruolo di supremazia della PA è, ad esempio, facilmente individuabile nel potere della stessa di rilasciare ‘concessioni’ ai privati. Alla luce di queste considerazioni, possono essere qualificati come ‘*pubblici ufficiali*’ tutti i soggetti preposti ad esplicare tale potere;
- il *potere certificativo* viene normalmente riconosciuto in quello di rappresentare come certa una determinata situazione sottoposta alla cognizione di un ‘pubblico agente’. Anche questa attività di certificazione pubblica è stata interpretata in senso assai lato, tanto da riconoscere nella stessa, non solo il potere certificativo *fidefacente*, ma una vera e propria dichiarazione di volontà della Pubblica Amministrazione.

Diversamente, deve invece considerarsi incaricato di pubblico servizio (art. 358 c.p.) chi, pur agendo nell’ambito di un’attività disciplinata nelle stesse forme della pubblica funzione, manca dei poteri tipici di quest’ultima, purché non svolga semplici mansioni di ordine né presti opera meramente materiale.

Come precisato dalla giurisprudenza prevalente, ai fini della individuazione della qualità di pubblico ufficiale o di incaricato di pubblico servizio, occorre verificare se la relativa attività sia disciplinata da norme di diritto pubblico e sia volta in concreto al perseguimento di interessi collettivi, restando irrilevanti la qualificazione e l’assetto formale dell’Ente per il quale il soggetto presta la propria opera.

Esempi di incaricati di un pubblico servizio sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati.

L’effettiva ricorrenza dei su indicati requisiti deve essere verificata, caso per caso, in ragione della concreta ed effettiva possibilità di ricondurre l’attività di interesse alle richiamate definizioni, essendo certamente ipotizzabile anche che soggetti appartenenti alla medesima categoria, ma addetti ad espletare differenti *funzioni* o *servizi*, possano essere diversamente qualificati proprio in ragione della non coincidenza dell’attività da loro in concreto svolta.

Sulla base di tale nozione sono state analizzate le situazioni di possibili rapporti con:

- a) soggetti che svolgono una pubblica funzione legislativa, quali ad esempio:
 - *parlamentari e membri del governo;*
 - *consiglieri regionali e provinciali;*
 - *parlamentari europei e membri del Consiglio d’Europa;*
 - *soggetti che svolgono funzioni accessorie* (addetti alla conservazione di atti e documenti parlamentari, alla redazione di resoconti stenografici, di economato, tecnici, etc.)
- b) soggetti che svolgono una pubblica funzione giudiziaria, quali ad esempio:
 - *magistrati* (magistratura ordinaria di Tribunali, Corti d’Appello, Suprema Corte di Cassazione, Tribunale Superiore delle Acque, TAR, Consiglio di Stato, Corte

Costituzionale, Tribunali Militari, giudici popolari delle Corti d'Assise, Giudici di pace, Vice Pretori Onorari ed aggregati, membri di collegi arbitrali rituali e di commissioni parlamentari d'inchiesta, magistrati della Corte Europea di Giustizia, nonché delle varie Corti internazionali, etc.);

- *soggetti che svolgono funzioni collegate* (ufficiali e agenti di polizia giudiziaria, guardia di finanza e carabinieri, cancellieri, segretari, custodi giudiziari, ufficiali giudiziari, messi di conciliazione, curatori fallimentari, operatori addetti al rilascio di certificati presso le cancellerie dei Tribunali, periti e consulenti del Pubblico Ministero, commissari liquidatori nelle procedure fallimentari, liquidatori del concordato preventivo, commissari straordinari dell'amministrazione straordinaria delle grandi imprese in crisi, etc.);
- c) soggetti che svolgono una pubblica funzione amministrativa, quali, ad esempio:
- *dipendenti, funzionari ed esponenti dello Stato, di organismi internazionali ed esteri e degli enti territoriali* (ad esempio funzionari e dipendenti dello Stato, dell'Unione europea, di organismi sopranazionali, di Stati esteri e degli enti territoriali, ivi comprese le Regioni, le Province, i Comuni e le Comunità montane; soggetti che svolgono funzioni accessorie rispetto ai fini istituzionali dello Stato, quali componenti dell'ufficio tecnico comunale, membri della commissione edilizia, capo ufficio amministrativo dell'ufficio condoni, messi comunali, addetti alle pratiche riguardanti l'occupazione del suolo pubblico, corrispondenti comunali addetti all'ufficio di collocamento, dipendenti delle aziende di Stato e delle aziende municipalizzate; soggetti addetti all'esazione dei tributi, personale sanitario delle strutture pubbliche, personale dei ministeri, delle soprintendenze, etc.);
 - *dipendenti di altri enti pubblici, nazionali ed internazionali* (ad esempio funzionari e dipendenti della Camera di Commercio, della Banca d'Italia, delle Cdatorità di vigilanza, degli istituti di previdenza pubblica, dell'AIFA ed EMEA, dell'ISTAT, dell'ONU, della FAO, etc.);
 - *privati esercenti pubbliche funzioni o pubblici servizi* (ad esempio notai, soggetti privati operanti in regime di concessione o la cui attività sia comunque regolata da norme di diritto pubblico e atti Cdatoritativi).

Occorre inoltre evidenziare che, a norma dell'art. 322-bis c.p., alla Pubblica Amministrazione così come sopra descritta si considera equiparata quella che svolga funzioni analoghe a quelle indicate nell'ambito di organismi comunitari, di altri Stati membri dell'Unione europea, di Stati esteri o organizzazioni pubbliche internazionali.

1.2 Descrizione delle singole fattispecie

1.2.1 Truffa aggravata in danno dello Stato o di altro ente pubblico (art. 640, comma 2 n. 1, c.p.)

Il reato si configura qualora, utilizzando artifici o raggiri ed in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro Ente pubblico o delle Comunità Europee.

Per 'artificio' o 'raggiri' si intende la simulazione o dissimulazione della realtà, atta ad indurre in errore una persona per effetto della percezione di una falsa apparenza. Il silenzio può integrare la condotta della truffa se attuata in presenza di un obbligo giuridico di comunicazione, anche di carattere extrapenale.

L'atto di disposizione del soggetto indotto in errore può comprendere ogni comportamento dotato di una efficacia in fatto; tale può essere considerata anche la semplice inerzia.

Il 'profitto' si ravvisa anche nella mancata diminuzione del patrimonio, per effetto, ad es., del godimento di un bene e, quindi, anche in assenza di un Cdamento effettivo di ricchezza; può anche non essere di natura patrimoniale, potendo consistere nel soddisfacimento di un interesse di natura morale.

A titolo meramente esemplificativo, il reato potrebbe configurarsi nel caso in cui si consegua l'aggiudicazione di gara pubblica mediante la falsificazione dei documenti inerenti le caratteristiche dei prodotti SILAQ SERVICE S.R.L., ovvero dei dati attestanti la sussistenza dei requisiti previsti per la partecipazione ad una gara e/o l'aggiudicazione della gara stessa.

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

Il reato si configura qualora la condotta di truffa sopra descritta sia posta in essere per conseguire indebitamente erogazioni pubbliche.

L'elemento qualificante rispetto al precedente reato è costituito dall'oggetto materiale della frode, in quanto per 'erogazione pubblica' si intende ogni attribuzione economica agevolata, erogata da parte dello Stato, di enti pubblici o delle Comunità europee.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si consegua un finanziamento o un contributo pubblico mediante il compimento di artifici e raggiri, come specificati nel punto precedente.

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

Il reato si configura qualora, dopo aver ricevuto da parte dello Stato italiano, di altro Ente pubblico o delle Comunità europee, finanziamenti, sovvenzioni o contributi destinati alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non si proceda all'utilizzo o alla destinazione delle somme ottenute per gli scopi cui erano originariamente destinate.

In concreto, occorre che le attribuzioni in denaro siano state distratte, anche parzialmente, senza che rilevi che l'attività programmata sia stata comunque realizzata.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui, a seguito della percezione di un finanziamento pubblico erogato per determinati fini, si ometta di destinare le somme percepite per tali finalità.

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

Il reato si configura allorquando, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi ovvero mediante l'omissione di informazioni dovute, si ottengano, pur senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.

In questa fattispecie, diversamente da quanto accade nel reato di malversazione in danno dello Stato e o di altro Ente pubblico (art. 316 *bis* cod. pen.), non ha alcuna rilevanza l'uso che viene fatto delle erogazioni, perfezionandosi il reato con il solo ottenimento degli indebiti finanziamenti.

Tale ipotesi di reato assume natura residuale rispetto alla più grave fattispecie di truffa in danno dello Stato (*ex art. 640, II comma, n. 1 cod. pen.*), per la cui sussistenza è necessaria l'induzione in errore mediante artifici o raggiri.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui il finanziamento venga concesso a seguito dell'utilizzazione di documenti falsi.

1.2.5 Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter, comma 1, 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 allo Stato o ad altro ente pubblico.

In concreto, il reato in esame potrebbe configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto.

1.2.6 Concussione (art. 317 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua qualità o del suo potere, costringa o induca taluno a dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità.

Il reato in esame presenta profili di rischio contenuti ai fini del D.Lgs. 231/01: trattandosi infatti di un reato proprio di soggetti qualificati, la responsabilità dell'ente potrà ravvisarsi solo nei casi in cui un Dipendente od un Agente della Società, nell'interesse o a vantaggio della stessa, *concorra* nel reato del pubblico ufficiale o dell'incaricato di pubblico servizio, che, approfittando della loro posizione, esigano prestazioni non dovute.

1.2.7 Corruzione

a) Corruzione per un atto d'ufficio (art. 318 cod. pen.)

Il reato si configura allorché un pubblico ufficiale (di seguito, per brevità, 'PU') o un incaricato di pubblico servizio (di seguito, per brevità, 'IPS') ricevano per sé o per altri, in denaro o altra utilità, una retribuzione non dovuta per compiere, o per aver compiuto, un atto del proprio ufficio.

Ai fini della ricorrenza di tale reato è necessario che la promessa di denaro o di altra utilità siano accettate dal PU, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 cod. pen. (su cui, vedi *infra*).

Il delitto di corruzione si differenzia da quello di 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 di pubblico servizio.

b) Corruzione per un atto contrario ai doveri d'ufficio (art. 319 cod. pen.)

Il reato si configura allorché un PU o un IPS ricevano per sé o per altri, in denaro o altra utilità, una retribuzione non dovuta per compiere, o per aver compiuto, un atto contrario ai doveri d'ufficio, ovvero per omettere o ritardare (o per avere omesso o ritardato) un atto del proprio ufficio.

E' necessario che la promessa di denaro o di altra utilità siano accettate dal PU, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 cod. pen. (su cui, vedi *infra*).

c) Corruzione in atti giudiziari (art. 319 *ter* cod. pen.)

Il reato si configura nel caso in cui i fatti di corruzione di cui alle fattispecie che precedono siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

E' opportuno evidenziare che nella nozione di PU sono sussumibili, oltre al magistrato, anche altri soggetti quali il cancelliere, i testi e qualsiasi altro funzionario pubblico operante nell'ambito di un contenzioso.

d) Corruzione di persone incaricate di un pubblico servizio (art. 320 cod. pen.)

Le disposizioni previste per il reato di corruzione per un atto contrario ai doveri di ufficio si applicano non solo al pubblico ufficiale bensì anche all'incaricato di pubblico servizio.

L'incaricato di pubblico servizio, inoltre, soggiacerà alle norme in materia di corruzione per un atto d'ufficio qualora rivesta la qualità di pubblico impiegato.

Per quanto concerne le ipotetiche modalità di attuazione del reato, quindi, si rimanda ai punti che hanno preceduto.

I reati di corruzione indicati sub punti a), b) c) e d), possono essere realizzati mediante l'erogazione di denaro o la promessa di erogazione di denaro al pubblico ufficiale/incaricato di pubblico servizio, la cui provvista derivi:

- dalla creazione di fondi occulti tramite l'emissione di fatture relative ad operazioni inesistenti;
- da rimborsi spese fittizi o per ammontare diverso da quello delle spese effettivamente sostenute anche attraverso consulenti;
- dall'utilizzo delle deleghe di spesa attribuite.

Sotto un diverso profilo, i reati di cui ai punti a), b), c) e d) possono essere realizzati mediante l'erogazione o la promessa di erogazione al pubblico ufficiale/incaricato di pubblico servizio di una qualsiasi altra utilità o retribuzione, quali in via esemplificativa:

- omaggi e, in genere, regalie;
- dazione/conferimento di beni a condizioni più favorevoli rispetto a quelle di mercato;
- assunzione di personale indicato dal pubblico ufficiale o incaricato di pubblico servizio;
- raggiungimento di accordi/sottoscrizione di lettere di incarico in favore di persone segnalate dal pubblico ufficiale o dall'incaricato di pubblico servizio a condizioni ingiustamente vantaggiose;
- cancellazione immotivata (totale o parziale) di un debito residuo dell'Ente presso cui il pubblico ufficiale/incaricato di pubblico servizio presta il suo servizio o di cui è rappresentante nei confronti della società, ecc.

A titolo esemplificativo, nei casi a), b) ed), il reato potrebbe essere finalizzato ad ottenere:

- il rilascio di una Cdatorizzazione alla immissione in commercio di un farmaco;
- un Cdamento indebito – da parte dei medici - delle prescrizioni di prodotti SILAQ SERVICE S.R.L.;
- l'aggiudicazione di una gara pubblica;

- un provvedimento Cdatorizzativo;
- la concessione/rilascio di una licenza;
- che i prodotti della società vengano preferiti ingiustamente – nell’acquisto o nella vendita - rispetto a quelli delle altre Società concorrenti.

In particolare, nel caso sub punto c), il fine del reato potrebbe essere quello di ottenere una pronuncia favorevole alla Società nell’ambito di un contenzioso.

Infine, per completezza, deve ricordarsi che, essendo i delitti di corruzione fattispecie a c.d. concorso necessario, ai sensi dell’art. 321 cod. pen., le pene stabilite agli artt. 318, 319, 319 *ter* e 320 cod. pen. si applicano anche al corruttore e non solo al corrotto.

1.2.8 Istigazione alla corruzione (art. 322 c.p.)

La pena prevista per tale reato si applica a chiunque offra o prometta denaro ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per indurlo a compiere un atto contrario o conforme ai doveri d’ufficio, qualora la promessa o l’offerta non vengano accettate.

Parimenti, si sanziona la condotta del pubblico agente che solleciti una promessa o un’offerta da parte di un privato.

1.2.9 Peculato, concussione, corruzione ed istigazione alla corruzione di membri degli Organi delle Comunità Europee o di Stati esteri (art. 322 bis cod. pen.)

Il reato si configura allorché la medesima condotta prevista per alcuno dei reati indicati in rubrica venga compiuta da, o nei confronti di, membri degli organi delle Comunità europee o di Stati esteri.

Tali soggetti sono assimilati ai pubblici ufficiali qualora esercitino funzioni corrispondenti, e agli incaricati di pubblico servizio negli altri casi.

Quanto alle possibili modalità di commissione del reato, si rinvia alle ipotesi previste, a titolo esemplificativo, per i reati di corruzione e concussione, fermo restando che, ai fini della configurabilità della fattispecie di istigazione, è necessario che l’offerta o la promessa non siano accettate.

1.2.10 Confisca (art. 322-ter)

La norma prevede che nel caso di condanna o di sentenza di “patteggiamento” per uno dei delitti previsti dagli articoli da 314 a 320 del codice penale, è sempre ordinata la confisca dei beni che ne costituiscono il profitto o il prezzo. La confisca è prevista anche “per equivalente”, ovverosia per un valore corrispondente a tale prezzo.

1.2.11 Inosservanza delle sanzioni interdittive (art. 23 D.Lgs. 231/2001)

Tale reato si realizza qualora, nello svolgimento dell’attività dell’Ente cui è stata applicata una sanzione o una misura cCdatelare interdittiva, si trasgredisca agli obblighi o ai divieti inerenti tali sanzioni o misure.

Inoltre, se dalla commissione del predetto reato l’Ente trae un profitto di rilevante entità, è prevista l’applicazione di misure interdittive anche differenti, ed ulteriori, rispetto a quelle già irrogate.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui la Società, pur soggiacendo alla misura interdittiva del divieto di contrattare con la Pubblica Amministrazione, partecipi ad una gara pubblica.

2. DESTINATARI DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere da Amministratori, Direttori Generali, Dirigenti e Dipendenti (collettivamente, “Esponenti Aziendali”, di cui all’organigramma allegato) operanti nelle aree di attività a rischio, nonché da collaboratori esterni, consulenti, liberi professionisti e *partners* d’affari (collettivamente “Collaboratori e Partners”) che, operando a qualsiasi titolo nelle aree a rischio di cui al successivo paragrafo 3, possono commettere o agevolare la commissione dei reati di cui alla presente Parte Speciale. E’ pertanto, in termini generali, fatto divieto ai suddetti collaboratori esterni e *partners* di subdelegare o subappaltare o comunque di conferire ad altri, salvo espresso consenso di SILAQ SERVICE S.R.L. che si riserva la scelta ed il controllo in ordine all’idoneità morale e professionale dei soggetti interessati, appalti, servizi, consulenze, ecc.

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 prevenire ed impedire il verificarsi dei reati che ne formano oggetto.

3. AREE POTENZIALMENTE ‘A RISCHIO’. ATTIVITÀ ‘SENSIBILI’. REATI PROSPETTABILI.

In occasione dell’implementazione dell’attività di *risk mapping*, sono state individuate, nell’ambito della struttura organizzativa ed aziendale di SILAQ SERVICE S.R.L., delle aree considerate ‘a rischio’, ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati contro la Pubblica Amministrazione.

Nell’ambito di ciascuna area ‘a rischio’, inoltre, sono state individuate le relative attività cd. ‘sensibili’, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in considerazione della sussistenza di rapporti diretti con gli organismi pubblici e/o i soggetti sopra individuati. Sono stati, infine, individuati i principali controlli che insistono su ciascuna area a rischio.

In relazione alle aree ‘a rischio’ si segnala che la società è dotata di un sistema di procedure operative standard sui seguenti temi:

- spese di rappresentanza (in particolare, pranzi e/o cene offerte) e sull’Omaggistica;
- Congressi – Convegni e Corsi di Aggiornamento;
- Donazioni – Atti di liberalità e Borse di Studio (con particolare riferimento a donazioni di beni strumentali e borse di studio);
- Contratti di consulenza e Lettere di incarico.

Di seguito è riepilogato il quadro in precedenza esposto.

Area a rischio n. 1: Stipulazione ed esecuzione di contratti di consulenza e collaborazione con 'opinion leaders'

Attività sensibili e reati astrattamente ipotizzabili

a) Conclusione di un contratto avente ad oggetto il conferimento di un incarico di collaborazione e/o consulenza per iniziative scientifiche e/o prestazioni di servizi

1) *Corruzione (artt. 318, 319, 320, 321, 322, 322 cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*

b) Gestione dei rapporti con soggetti pubblici ovvero incaricati di pubblico servizio nell'ambito delle attività di comunicazione/diffusione di fatti e dati riguardanti le attività di ricerca della Società

1) *Corruzione (artt. 318, 319, 319, 320, 321, 322 cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nello svolgimento del processo di stipulazione ed esecuzione di contratti sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. formalizzazione della motivazione al fine di documentare e rendere trasparenti i motivi dell'attivazione della consulenza ed i criteri di scelta del consulente/opinion leader. In particolare, l'aspetto decisionale delle iniziative in esame è riservato esclusivamente ai vertici operativi aziendali e il consulente/opinion leader deve essere soggetto di comprovata affidabilità e di levatura nazionale;
2. adozione ed utilizzo di un tariffario standard per la definizione del compenso da corrispondere al consulente;
3. inserimento nel contratto di consulenza della clCdasola di rispetto del Codice Etico adottato da SILAQ SERVICE S.R.L., al fine di sanzionare eventuali comportamenti/condotte contrari ai principi etici;
4. evidenza documentale del controllo sulla prestazione ricevuta, prima del benestare al pagamento, al fine di verificare la conformità al contratto e la qualità di quanto prodotto;
5. evidenza documentale relativa all'ottenimento, da parte del consulente o opinion leader, dell' autorizzazione dell'Ente di appartenenza;
6. nel caso in cui non sia possibile procedere secondo le modalità di cui al punto precedente, il contratto è stipulato direttamente con l'Ente di appartenenza del consulente o opinion leader;

Area a rischio n. 2: Elargizioni ed altre iniziative liberali

Attività sensibili e reati astrattamente ipotizzabili

a) Elargizioni e, in genere, iniziative di carattere liberale in favore di Enti Pubblici, Società Scientifiche, Fondazioni ed Associazioni attuate mediante: individuazione degli Enti Pubblici, Società Scientifiche, Fondazioni ed Associazioni.

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nello svolgimento del processo di erogazione di elargizioni ed altre iniziative liberali sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. destinatari delle elargizioni e delle altre iniziative liberali sono esclusivamente Enti di provata affidabilità e di levatura nazionale, di cui sia ben nota la missione;
2. evidenza formale della lettera di richiesta e dell'accettazione della delibera (o altro documento equivalente) da parte dell'Ente beneficiario;
3. evidenza formale della documentazione di supporto alla richiesta di contributo da parte dell'Ente beneficiario;
4. approvazione dell'iniziativa, nel rispetto del principio di segregazione delle funzioni, da parte del *Management*;
5. verifica dell'utilizzo e della destinazione del contributo erogato, tramite lettera di feed-back da parte dell'Ente beneficiario, necessaria per la registrazione a sistema della consuntivazione dell'elargizione;
7. il numero di elargizioni a favore di un singolo Ente non può essere superiore a tre per ogni anno e non può superare complessivamente l'importo massimo di Euro 15.000;
8. le elargizioni possono essere erogate esclusivamente ad Enti, comunque denominati, che perseguano finalità di studio, cura o assistenza sulle problematiche legate alla Sicurezza sul Lavoro.

Area a rischio n. 3: Gestione gare e procedure negoziate

Attività sensibili e reati astrattamente ipotizzabili

a) Contatto tra i rappresentanti della società e della PA al fine di ottenere chiarimenti o specificazioni in ordine alla gara/procedura negoziata

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*

3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

b) Predisposizione della documentazione e successivo invio della stessa per la partecipazione alla gara/procedura negoziata

1) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

c) Aggiudicazione gara: predisposizione della documentazione amministrativa richiesta ed invio all'Ente pubblico

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*

3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio gestione gare e procedure negoziate/vendite alle P.A. sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure

aziendali emesse a regolamentazione di tale area a rischio.

Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. formalizzazione dell'analisi di fattibilità effettuata dal Sales & Marketing Director con l'adesione delle altre Direzioni, al fine di verificare il possesso da parte di SILAQ SERVICE S.R.L. dei requisiti indicati nel bando di gara;
2. individuazione chiara del soggetto aziendale responsabile del controllo della completezza e correttezza della documentazione da inviare all'Ente appaltante per la partecipazione alla gara ed evidenza dell'approvazione;
3. accesso ristretto a determinati soggetti aziendali, chiaramente identificati, al sistema informatico utilizzato per la predisposizione dell'offerta di gara, al fine di impedire manipolazioni dei dati da trasmettere all'Ente appaltante;
4. controllo formale di conformità delle condizioni e dei termini della delibera di aggiudicazione con quanto previsto in fase di approvazione delle offerte;
5. definizione delle responsabilità dei soggetti coinvolti nel processo di partecipazione alle gare pubbliche (approvazione ed l'invio all'Ente della documentazione necessaria ai fini della definizione delle Offerte; definizione dei prezzi; rappresentanza della società nei contatti diretti con l'Ente appaltante- es. apertura delle buste) nel rispetto del principio di segregazione delle funzioni.

Area a rischio n. 4: Gestione congressi/ convegni/ seminari/ investigator meetings

Attività sensibili e reati astrattamente ipotizzabili

a) Gestione degli adempimenti relativi all'organizzazione di congressi, convegni, seminari, investigator meetings

- 1) *Corruzione (artt. 318, 319, 320, 321, 322 cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

b) Gestione dei rapporti con funzionari Pubblici in occasione di visite/ ispezioni per la verifica degli adempimenti di legge

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, cod. pen.)*

c) Sponsorizzazione di eventi di divulgazione tecnico/scientifica organizzati dalla Pubblica Amministrazione

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

d) Contatto con il Pubblico Ufficiale o incaricato di Pubblico Servizio diretto all'eventuale coinvolgimento in iniziative congressuali, convegni, seminari, *investigator meetings*

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio gestione di congressi/ convegni/ seminari sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. definizione di regole stringenti da rispettare nell'organizzazione dell'evento, relativamente a località, sede congressuale prescelta, durata dell'ospitalità, attinenza target invitati-argomento trattato, partecipazione di soggetti stranieri, al fine di assicurare il rispetto dei vincoli normativi ed evitare il cd. 'turismo congressuale':

- a) non è consentito invitare lo stesso soggetto a congressi, convegni, riunioni scientifiche e visite agli uffici aziendali più di due volte l'anno. Quest'ultimo limite non si applica ai relatori e moderatori;
- b) non è consentita la realizzazione all'estero di convegni e congressi organizzati direttamente o indirettamente dall'azienda e a cui partecipino prevalentemente medici italiani;
- c) in nessun caso è consentita l'organizzazione di iniziative aventi anche finalità di tipo turistico;
- d) l'invito a convegni e congressi, è subordinato all'esistenza di una specifica attinenza tra la tematica oggetto della manifestazione congressuale e la specializzazione partecipanti;
- e) le manifestazioni organizzate direttamente o indirettamente da SILAQ SERVICE S.R.L. devono tenersi in località e sedi la cui scelta sia motivata da ragioni di carattere logistico, scientifico ed organizzativo, con esclusione di luoghi destinati alla ristorazione, ed essere caratterizzate da un programma scientifico qualificante. L'ambito territoriale di provenienza dei partecipanti dovrà essere di livello internazionale, nazionale o almeno regionale. Sono tassativamente escluse località a carattere esclusivamente turistico nel periodo 1° giugno – 30 settembre per le località di mare e 1° dicembre – 31 marzo e 1° luglio – 31 agosto per le località di montagna;
- f) nell'ambito delle manifestazioni nazionali e regionali è fatto divieto di organizzare o sponsorizzare iniziative di tipo sociale, culturale o turistico e cene di gala. Sono invece consentite le cene sociali organizzate dal Congresso per la collegialità dei partecipanti e comprese nella quota di iscrizione al Congresso stesso. E' inoltre esclusa l'ospitalità per accompagnatori a qualsiasi livello e sotto qualsiasi forma;

2. possibilità di sponsorizzare eventi congressuali;

3. selezione dei fornitori effettuata da due soggetti aziendali distinti (per la parte scientifica l'*initiator* del *meeting* e per la parte logistica l'ufficio Acquisti) ed in base a criteri definiti a priori;

4. evidenza documentale del processo di gara/selezione dei fornitori utilizzati, al fine di garantire la trasparenza dell'assegnazione dell'incarico;

5. inserimento nel contratto con i provider/fornitori della clCdasola di rispetto del Codice Etico adottato da SILAQ SERVICE S.R.L., al fine di sanzionare eventuali comportamenti/condotte contrari ai principi etici;

6. necessità di Cdatorizzazione formale di eventuali spese extra (rispetto al preventivo approvato) sostenute nel corso dell'iniziativa congressuale e controlli delle spese a consuntivo al fine di portare all'attenzione del *Management* eventuali scostamenti rilevanti rispetto al preventivo, che possano falsare i criteri di aggiudicazione della gara;

7. evidenza documentale del pagamento del relatore da parte dell'amministrazione;

8. omogeneità dei compensi ai medici/relatori in relazione al medesimo evento;

Area a rischio n. 5: Studi osservazionali

Attività sensibili e reati astrattamente ipotizzabili

a) Contatto con i rappresentanti di un Ente a rilevanza pubblicistica al fine di identificare gli obiettivi dello studio e le condizioni necessarie al raggiungimento dello scopo dello stesso

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110, cod. pen.)*

b) Predisposizione del protocollo per la conduzione dello studio, in collaborazione con l'Ente di ricerca e contatto con il comitato etico per ottenere l'approvazione dello stesso

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio studi osservazionali sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. effettuazione di una serie di verifiche sui requisiti dei centri da arruolare per la conduzione dello studio in termini di adeguatezza della sede, della struttura e delle qualifiche dello sperimentatore e del suo staff, al fine di garantire la fattibilità dello studio presso gli stessi e la trasparenza dei criteri di selezione dei centri sperimentali;

2. controlli di accuratezza e completezza della documentazione presentata alle Cdatorità regolatorie per l'ottenimento dell'Cdatorizzazione alla conduzione dello studio;

Area a rischio n. 6: ambiente, salute e sicurezza, limitatamente ai rapporti con la p.a.

Attività sensibili e reati astrattamente ipotizzabili

a) Gestione degli adempimenti e della relativa documentazione ex D.Lgs. 81/08 e s.m.i. (es. tenuta registro infortuni, comunicazione periodica della relazione sull'andamento degli infortuni e delle malattie professionali, ecc.)

1) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, cod. pen., art. 110 cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

b) Gestione documentazione relativa agli adempimenti ambientali e alle attività legate allo smaltimento dei rifiuti

1) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

c) Gestione dei rapporti con la PA in caso di verifiche ed ispezioni volte ad accertare l'osservanza delle prescrizioni di cui alla Legge 626/94, delle norme igienico-sanitarie e delle norme ambientali

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comm 2 cod. pen., art. 110 cod. pen.)*

3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2 cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio ambiente, salute e sicurezza sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. chiara identificazione dei soggetti aziendali responsabili degli adempimenti in materia di ambiente, salute e sicurezza ed autorizzati a rappresentare l'azienda nei rapporti con le autorità competenti;
2. formalizzazione dei contatti avuti con la PA, in sede di verifica degli adempimenti di legge in materia di ambiente, salute e sicurezza;
3. monitoraggio, tramite scadenziari, degli adempimenti previsti in materia di ambiente, salute e sicurezza, al fine di garantire il rispetto dei termini di legge;
4. rispetto delle procedure e delle attività delineate nella Parte Speciale E in tema di salute e sicurezza del lavoro.

Si ricorda, infine, che la società ha adottato il documento di valutazione dei rischi D. Lgs. 81/2008.

Area a rischio n. 7: gestione rapporti con p.a. per adempimenti amministrazione del personale

Attività sensibili e reati astrattamente ipotizzabili

a) Predisposizione e trasmissione e, comunque, contatto con agli organi competenti della documentazione necessaria all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

b) Verifiche dei funzionari pubblici circa il rispetto delle condizioni richieste dalla legge per l'assunzione agevolata di personale o assunzione di personale appartenente alle categorie protette

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

c) Gestione dei rapporti con gli organi competenti in materia di infortuni, malattie sul lavoro, assunzioni del rapporto di lavoro

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

d) Compilazione delle dichiarazioni contributive, fiscali e versamento dei contributi previdenziali ed erariali

- 1) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*
- 2) *Frode informatica a danno dello Stato o di un altro Ente pubblico (art. 640 ter, cod. pen.)*

e) Gestione rapporti con gli organi competenti in caso di ispezioni/accertamenti effettuati dai funzionari pubblici

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio gestione di rapporti con la PA per adempimenti amministrazione del personale sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. gestione centralizzata dei rapporti con gli enti pubblici competenti in materia di adempimenti legati al Personale;
2. chiara identificazione del soggetto responsabile di effettuare il controllo di accuratezza e completezza dei dati inviati alla PA;
3. segregazione di funzioni tra chi predispone la documentazione da inviare alla PA e chi la controlla prima dell'invio;
4. monitoraggio delle scadenze da rispettare per le comunicazioni/denunce/adempimenti nei confronti degli enti pubblici competenti, tramite scadenziari e timetable inviate alle funzioni aziendali coinvolte per la raccolta e consolidamento dei dati.

Area a rischio n. 8: gestione rapporti con l' Cdatorità garante della privacy

Attività sensibili e reati astrattamente ipotizzabili

a) Raccolta e trasmissione di dati, informazioni e documenti all' Cdatorità Garante della Privacy

- 1) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*
- 2) *Frode informatica a danno dello Stato o di un altro Ente pubblico (art. 640 ter, cod. pen.)*

b) Gestione dei rapporti con il Garante della Privacy e con l'Ufficio del Garante in occasione di ispezioni e controlli disposti dall' Cdatorità Garante della Privacy

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio gestione dei rapporti con l' Cdatorità Garante della Privacy sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. chiara identificazione dei soggetti aziendali responsabili del trattamento dei dati personali ed Cdatorizzati a rappresentare l'azienda nei rapporti con l' Cdatorità Garante della Privacy;
2. formalizzazione dei contatti/rapporti intercorsi con l' Cdatorità Garante della Privacy;

3. verifiche periodiche formalizzate da parte del Titolare Trattamento Dati Personali sulla puntuale osservanza delle disposizioni di legge;
4. accesso ai dati sensibili (archivi fisici ed elettronici) limitato alle sole persone Cdatorizzate;
5. controlli di accuratezza e completezza della documentazione/dati trasmessi all'Cdatorità di vigilanza.

La società ha adottato il documento programmatico per la sicurezza ai sensi del Regolamento Europeo in materia di protezione dei dati personali (GDPR in vigore dal 25.05.2018)

Area a rischio n. 9: gestione rapporti con amministrazione finanziaria

Attività sensibili e reati astrattamente ipotizzabili

a) Esecuzione dei versamenti relativi alle imposte dirette e indirette, predisposizione e trasmissione delle relative dichiarazioni

1) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod.pen.)*

2) *Frode informatica a danno dello Stato o di un altro Ente pubblico (art. 640 ter, cod.pen.)*

b) Rapporti con l'amministrazione finanziaria nel caso di ispezioni e controlli in materia fiscale

1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*

2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod.pen.)*

3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod.pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nel Codice Etico, i soggetti aziendali coinvolti nell'area a rischio gestione rapporti con l'amministrazione finanziaria sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. chiara identificazione dei soggetti aziendali Cdatorizzati a rappresentare l'azienda nei rapporti con l'amministrazione finanziaria;
2. formalizzazione dei rapporti intercorsi con la PA, in particolare in sede di verifiche ispettive;
3. monitoraggio dell'evoluzione del piano normativo di riferimento, effettuato con il supporto di consulenti esterni, al fine di garantire l'adeguamento alle nuove leggi in materia fiscale;
4. controlli di dettaglio per verificare la correttezza del calcolo delle imposte ed approvazione formale della documentazione a supporto;
5. monitoraggio costante attraverso uno scadenziario degli adempimenti di legge, al fine di evitare ritardi e imprecisioni nella presentazione di dichiarazioni e/o documenti fiscali;
6. reporting formalizzato e periodico all'Amministrazione sui rischi e sui contenziosi attualmente in corso sull'area Tax;
7. inserimento nel contratto con le società esterne della clCdasola di rispetto del Codice Etico adottato da SILAQ SERVICE S.R.L., al fine di sanzionare eventuali comportamenti/condotte contrari ai principi etici.

Area a rischio n. 10: richiesta e gestione di finanziamenti pubblici

Attività sensibili e reati astrattamente ipotizzabili

a) Presentazione della richiesta/domanda di finanziamento e della documentazione a supporto anche mediante consulenti esterni

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.);*
- 4) *truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis, comma 2, cod. pen.)*

b) Partecipazione a verifiche in sede da parte dell'Ente erogante sia in fase di realizzazione che a fine attività

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*

c) Utilizzo dei fondi ottenuti a mezzo del finanziamento e gestione di eventuali adeguamenti/aggiornamenti dell'attività oggetto del contratto di contributo/finanziamento agevolato

- 1) *Corruzione (artt. 318, 319, 320, 321, 322, cod. pen.)*
- 2) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen., art. 110 cod. pen.)*
- 3) *Truffa a danno dello Stato o di un altro Ente pubblico (art. 640, comma 2, cod. pen.)*
- 4) *Malversazione a danno dello Stato (art. 316 bis, cod. pen.)*
- 5) *Indebita percezione di erogazioni a danno dello Stato (art. 316 ter, cod. pen.)*

Controlli esistenti

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.) i soggetti aziendali coinvolti nell'area a rischio richiesta e gestione di finanziamenti pubblici sono tenuti, al fine di prevenire e impedire il verificarsi dei reati contro la P.A., al rispetto delle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. chiara identificazione dei soggetti aziendali Cdatorizzati a rappresentare l'azienda nei rapporti con la PA per la richiesta di finanziamenti agevolati;
2. segregazione di funzioni tra chi propone la richiesta di un finanziamento agevolato, chi effettua lo studio di fattibilità per valutare la possibilità di accedere al finanziamento, chi raccoglie e predispone la documentazione necessaria per la richiesta e chi approva e sottoscrive la richiesta;
3. controlli preventivi ed effettuazione di studi di fattibilità per la verifica del possesso dei requisiti/parametri richiesti dalla legge per l'ottenimento del finanziamento;
4. controlli sulla documentazione allegata alla richiesta di finanziamento al fine di garantire la completezza, accuratezza e veridicità dei dati comunicati alla PA;
5. monitoraggio periodico dei progetti coperti da finanziamenti pubblici allo scopo di garantire il persistere delle condizioni in base alle quali è stato ottenuto il finanziamento;

6. inserimento nel contratto con le società esterne, che supportano l'azienda nelle attività di richiesta dei finanziamenti agevolati, della clCdasola di rispetto del Codice Etico adottato da SILAQ SERVICE S.R.L., al fine di sanzionare eventuali comportamenti/condotte contrari ai principi etici.

4. I PRINCIPI GENERALI DI COMPORTAMENTO

I responsabili delle direzioni, delle funzioni e dei servizi coinvolti nelle aree a rischio e/o in quelle strumentali sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico di SILAQ SERVICE S.R.L., dal Manuale di Sistema ISO 9001:2008 contenenti le procedure adottate.

E' fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dagli artt. 24 e 25 del D.Lgs. 231/2001;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di porre in essere o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con la Società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della Società e nel pieno rispetto delle norme del Codice Etico;
- di elargire o promettere denaro a pubblici ufficiali o incaricati di pubblico servizio;
- di distribuire o promettere omaggi e regali che non siano di modico valore, in violazione di quanto previsto dal Codice Etico e dalla prassi aziendale;
- di accordare o promettere altri vantaggi, di qualsiasi natura essi siano, in favore di pubblici ufficiali o incaricati di pubblico servizio;
- con riguardo al settore vendite/commerciale, di porre in essere comportamenti o di realizzare iniziative - ivi inclusi il riconoscimento di incentivi di tipo economico o l'assegnazione di materiale didattico, scientifico o promozionale - non conformi alla Legge (ad es., disposizioni del D.Lgs. n. 219/2006) ed alle procedure aziendali vigenti, ovvero volti - o comunque potenzialmente idonei - ad influenzare la libera determinazione dei clienti;
- nell'ambito di convegni, congressi, corsi e riunioni, ed in genere nei rapporti con gli operatori del esterni, di porre in essere comportamenti o di realizzare iniziative non conformi alla Legge (ad es., disposizioni del D.Lgs. n. 219/2006) ed alle procedure aziendali vigenti, ovvero volti - o comunque potenzialmente idonei - a riconoscere, anche in via indiretta, vantaggi, utilità o trattamenti di favore indebiti;
- di effettuare prestazioni in favore dei Partner e/o dei consulenti e/o dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto associativo con essi costituito;
- di riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- di presentare dichiarazioni e/o documenti e/o dati e/o informazioni non rispondenti al vero o incompleti ad organismi pubblici nazionali, comunitari o esteri, tanto meno al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- di destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti, per scopi differenti da quelli cui erano destinati originariamente.

Inoltre, ai fini dell'attuazione dei comportamenti di cui sopra:

- occorre garantire il rispetto delle previsioni contenute nel Codice Etico di SILAQ SERVICE S.R.L.;
- nell'ambito dei rapporti con la Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio deve essere garantito il rispetto dei principi di correttezza, trasparenza e buona fede;
- nelle aree a rischio, i rapporti con soggetti qualificabili come pubblici ufficiali o incaricati di pubblico servizio devono essere gestiti in modo unitario;
- nell'ambito dell'attività commerciale, occorre adottare un comportamento improntato ai principi di integrità, onestà, trasparenza e buona fede;
- la partecipazione alle manifestazioni congressuali da parte della Società deve comunque essere connessa al ruolo da essa svolto nei settori della ricerca, dello sviluppo e della informazione scientifica, e deve essere ispirata a criteri di eticità, scientificità ed economicità;
- l'obiettivo primario della partecipazione o della organizzazione di convegni o congressi di livello nazionale e regionale deve essere indirizzato allo sviluppo della collaborazione con commercialisti e consulenti del lavoro;
- gli accordi di associazione con i Partner devono essere definiti per iscritto, ponendo in evidenza tutte le condizioni dell'accordo stesso - in particolare per quanto concerne le condizioni economiche concordate per la partecipazione congiunta alla procedura di gara;
- gli incarichi conferiti ai collaboratori esterni devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito, ed essere sottoscritti conformemente alle deleghe ricevute;
- nessun tipo di pagamento può essere effettuato in natura;
- le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
- coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi
- all'espletamento delle suddette attività devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.

5. IL RESPONSABILE INTERNO PER LE AREE A RISCHIO E LE SCHEDE DI EVIDENZA

In linea con le *best practice*, la Società ritiene opportuno che venga fornita debita evidenza delle operazioni a rischio.

A tal fine, in relazione alle aree a rischio diretto di reato, sono individuati e nominati da parte dell'OdV uno o più Responsabili Interni per ciascuna area, cui sarà richiesto di gestire il flusso informativo verso l'OdV in merito allo svolgimento delle attività aziendali.

L'OdV curerà l'emanazione e l'aggiornamento di istruzioni standardizzate relative alla compilazione omogenea e coerente degli strumenti di monitoraggio e delle evidenze che riterrà opportune.

6. I COMPITI DELL'ORGANISMO DI VIGILANZA

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'OdV nel documento approvato dall'Cda e denominato 'Disciplina e compiti dell'OdV', in relazione alla prevenzione dei reati di cui alla presente parte speciale, l'OdV, tra l'altro, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati contro la Pubblica Amministrazione, previsti dal D.Lgs. n. 231/2001;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi *sub* responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati contro la pubblica Amministrazione ed all'Cda, secondo i termini indicati nel documento "Disciplina e compiti dell'OdV".

PARTE SPECIALE “B”

REATI SOCIETARI

INDICE

1) LA TIPOLOGIA DEI REATI SOCIETARI (ART. 25-TER DEL DECRETO)

- 1.1) FALSITA' IN COMUNICAZIONI, PROSPETTI E RELAZIONI
- 1.2) TUTELA PENALE DEL CAPITALE SOCIALE
- 1.3) TUTELA PENALE DEL PATRIMONIO SOCIALE
- 1.4) TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETA'
- 1.5) TUTELA PENALE CONTRO LE FRODI
- 1.6) TUTELA PENALE DELLE FUNZIONI DI VIGILANZA
- 1.7) DISPOSIZIONI COMUNI FINALI.

2) DESTINATARI DELLA PARTE SPECIALE

3) PRINCIPALI AREE DI ATTIVITÀ A RISCHIO

4) PRINCIPI GENERALI DEI CONTROLLI ESISTENTI

5) PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

6) PRINCIPI DI ATTUAZIONE DEL MODELLO NELLE ATTIVITA' A RISCHIO

- 6.1) BILANCI ED ALTRE COMUNICAZIONI SOCIALI
- 6.2) TUTELA DEL CAPITALE SOCIALE
- 6.3) ATTIVITA' SOGGETTE A VIGILANZA
- 6.4) CONFLITTI DI INTERESSE

7) COMPITI DELL'ORGANISMO DI VIGILANZA

1) LA TIPOLOGIA DEI REATI SOCIETARI (ART. 25-TER DEL DECRETO)

La presente Parte Speciale è dedicata alla trattazione dei reati societari così come individuati dall'articolo 25-ter del Decreto Legislativo.

Il regime sanzionatorio applicabile all'Ente per i reati societari è di natura esclusivamente pecuniaria, non essendo previste sanzioni interdittive.

La Legge n. 262/2005 ha raddoppiato le sanzioni pecuniarie all'Ente previste dall'originario art. 25 ter del Decreto Legislativo.

1.1) FALSITA' IN COMUNICAZIONI, PROSPETTI E RELAZIONI

a) False comunicazioni sociali (artt. 2621 e 2622 c.c.)

Si tratta di due modalità di reato la cui condotta tipica coincide quasi totalmente e che si differenziano per il verificarsi o meno di un danno patrimoniale per la società, i soci o i creditori.

La prima (art. 2621 c.c.) è una fattispecie di pericolo ed è costruita come una contravvenzione dolosa; la seconda (art. 2622 c.c.) è costruita come un delitto di danno.

Le due fattispecie si realizzano con l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali che, ancorché oggetto di valutazioni, non siano veritieri e possano indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false 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 punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico d'esercizio al lordo delle imposte non superiore al 5% o una variazione del patrimonio netto non superiore all'1%; in ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate differiscono in misura non superiore al 10% di quella corretta;
- la responsabilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori (reato proprio).

b) Art. 2623 c.c. - Falso in prospetto.

L'art. 34 della legge 28 dicembre 2005 n. 262 ha abrogato l'art. 2623 c.c. ed ha contestualmente inserito il reato di "falso in prospetto" all'interno del D.Lgs. 24 febbraio 1998 n. 58 (art. 173-bis). In seguito alla citata traslazione, il reato non è più compreso nel novero delle fattispecie Cdatonomamente rilevanti ai fini dell'applicazione del D.Lgs. 231/01.

Le falsità nei prospetti informativi e negli altri documenti richiamati dall'abrogato art. 2623 c.c. possono peraltro ora assumere rilevanza quali "false comunicazioni sociali" di cui agli art. 2621 e 2622 c.c., qualora ricorrano tutti i presupposti richiesti da detti articoli.

c) Falsità nelle relazioni o nelle comunicazioni della Società di Revisione (art. 2624 c.c.)

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, concernenti la situazione economica patrimoniale o finanziaria della società, poste in essere al fine di conseguire per sé o per gli altri un ingiusto profitto e con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni.

A seconda che dalla stessa condotta intenzionale derivi o no l'evento materiale del danno patrimoniale ai destinatari delle comunicazioni, sono previste due distinte ipotesi di reato: una di natura contravvenzionale ed una di natura delittuosa.

Soggetti attivi sono i responsabili della revisione contabile (reato proprio), ma i componenti degli organi di amministrazione di SILAQ SERVICE S.R.L. ed i suoi dipendenti possono essere coinvolti a titolo di concorso nel reato. E', infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato, istigato, o comunque agevolato la condotta illecita del responsabile della revisione.

1.2) TUTELA PENALE DEL CAPITALE SOCIALE

a) Indebita restituzione dei conferimenti (art. 2626)

La condotta tipica consiste nella restituzione dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli, in maniera palese o simulata, fuori dei casi di legittima riduzione del capitale sociale.

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

b) Illegale ripartizione degli utili o delle riserve (2627 c.c.)

La condotta criminosa di tale reato, di natura contravvenzionale, consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Si fa presente che la ricostituzione degli utili o delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetti attivi del reato sono gli amministratori (reato proprio).

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

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

Si fa presente che se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Il reato può essere commesso dagli amministratori in relazione alle azioni della società.

d) 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 di capitale sociale, fusioni con altre società o scissioni, che cagionino danno ai creditori. Trattasi, dunque, di un reato di danno, procedibile a querela della persona offesa.

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

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

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

Il reato è integrato dalle seguenti condotte: a) fittizia formazione o Cdamento del capitale sociale mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; b) sottoscrizione reciproca di azioni o quote; c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi della società sono gli amministratori ed i soci conferenti.

Si precisa che non è, invece, incriminato l'omesso controllo ed eventuale revisione da parte di amministratori e sindaci, ai sensi dell'art. 2343, 3° comma, c.c. della valutazione dei conferimenti in natura contenuta nella relazione di stima redatta dall'esperto nominato dal Tribunale.

f) Indebita ripartizione dei beni sociali da parte dei liquidatori (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 (reato di danno).

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

Soggetti attivi del reato sono esclusivamente i liquidatori (reato proprio).

1.3) LA TUTELA PENALE DEL PATRIMONIO SOCIALE.

a) L'omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.).

L'art. 2629-bis c.c. (introdotto dalla legge n. 58/2005 in tema di tutela del risparmio), sanziona l'inosservanza dell'obbligo, da parte degli amministratori (o dei membri del consiglio di gestione), di comunicare al Organo Amministrativo ed al collegio sindacale l'interesse in una determinata operazione (ex art. 2391 c.c.) cui segua la verifica di un danno alla società o a terzi.

La portata applicativa della norma, tuttavia, è circoscritta agli amministratori (o componenti del consiglio di gestione) di società *quotate o con titoli diffusi* tra il pubblico in misura rilevante ex art. 116 t.u.f., nonché degli

enti *sottoposti a vigilanza* da parte di un'Ente di controllo individuati dal t.u.l.b., dal c.d. codice delle assicurazioni private e dalla disciplina in tema di fondi pensione.

1.4) TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETA'

a) Impedito controllo (art. 2625 c.c.)

La condotta incriminata consiste nell'ostacolare o impedire lo svolgimento delle attività di controllo e/o di revisione - legalmente attribuite ai soci, ad organi sociali o a società di revisione - attraverso l'occultamento di documenti od altri idonei artifici.

Il reato, che può essere commesso esclusivamente dagli amministratori, è punito più gravemente se la condotta ha causato un danno e se si tratta di società con titoli quotati in mercati regolamentati italiani od europei o diffusi tra il pubblico in misura rilevante.

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

La condotta illecita, che può essere posta in essere da chiunque, si perfeziona con la formazione irregolare di una maggioranza che altrimenti non si sarebbe avuta, ciò attraverso il compimento di atti simulati o frodolenti. E' necessario un concreto risultato lesivo, che sia strumentale al conseguimento della finalità espressa dal dolo specifico.

1.5) TUTELA PENALE CONTRO LE FRODI

a) Aggiotaggio (art. 2637 c.c.)

La realizzazione del reato avviene attraverso la diffusione di notizie false o attraverso il compimento di operazioni simulate od altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non sia stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

Anche questo è un reato comune che può essere commesso da chiunque.

La legge 28 dicembre 2005 n. 262 ha modificato la precedente fattispecie di cui all'art. 2637 c.c., limitando l'applicazione della medesima agli strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

La scelta del Legislatore nasce dal fatto di aver esso disciplinato la diversa fattispecie criminosa avente ad oggetto strumenti finanziari quotati, con la previsione dello specifico reato di manipolazione del mercato.

Il reato in esame si configura come fattispecie di pericolo concreto, in quanto è necessario che le notizie mendaci, o le operazioni simulate o gli altri artifici, siano concretamente idonee a provocare una effettiva lesione. Oggetto materiale del reato sono gli strumenti finanziari non quotati (o per i quali non è stata presentata richiesta di quotazione).

1.6) TUTELA PENALE DELLE FUNZIONI DI VIGILANZA

a) Ostacolo all'esercizio delle Cdatorità pubbliche di vigilanza (art. 2638 c.c.)

L'articolo prevede fattispecie delittuose diverse per modalità di condotta e momento offensivo: la prima centrata sul falso commesso al fine di ostacolare le funzioni di vigilanza; la seconda sulla realizzazione intenzionale dell'evento di ostacolo attraverso una qualsiasi condotta (attiva od omissiva).

Si precisa che:

- la prima ipotesi di reato si incentra su una condotta di falsità - o di occultamento di fatti che devono essere comunicati – sorretta dalla finalità specifica di ostacolare le funzioni di vigilanza (dolo specifico);
- la seconda ipotesi configura un reato di evento (ostacolo all'esercizio delle funzioni di vigilanza) a forma libera, realizzabile, cioè con qualsiasi modalità di condotta, inclusi i comportamenti omissivi, il cui elemento soggettivo è costituito dal dolo generico.

In entrambe le modalità descritte i soggetti attivi nella realizzazione del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili, i sindaci e i liquidatori.

1.7) DISPOSIZIONI COMUNI FINALI.

a) Estensione delle qualifiche soggettive (art. 2639 c.c.)

Destinatari della presente Parte Speciale “B” sono gli amministratori, i sindaci (se presenti), i direttori generali, i liquidatori (c.d. soggetti ‘apicali’), nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio.

Per i reati descritti il legislatore equipara al soggetto formalmente investito della qualifica o titolare della funzione prevista dalla legge civile, sia chi è tenuto a svolgere la stessa funzione diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Fuori dei casi di applicazione delle norme riguardanti i delitti dei pubblici ufficiali contro la pubblica amministrazione, le disposizioni sanzionatorie relative agli amministratori si applicano anche a coloro che sono legalmente incaricati dall'Cdatorità giudiziaria o dall'Cdatorità pubblica di vigilanza di amministrare la società o i beni dalla stessa posseduti o gestiti per conto di terzi.

b) Delitti tentati (art. 26).

Le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà in relazione alla commissione, nelle forme del tentativo, dei delitti indicati nel presente capo del decreto.

L'ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

c) Profitto di rilevante entità (art. 25-ter, co. 2).

Se, in seguito alla commissione dei reati di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è Cdamentata di un terzo.

2) DESTINATARI DELLA PARTE SPECIALE

L'art. 25-ter non si è uniformato alla tecnica descrittiva del d.lgs. n. 231/2001, limitandosi ad elencare le fattispecie e rinviando, per il resto, alla parte generale del decreto stesso; al contrario, esso elenca *ex novo* i soggetti e pure i criteri d'imputazione.

Pertanto, si rammenta che destinatari della presente Parte Speciale "B" sono gli amministratori, i direttori generali o *managers*, i liquidatori (c.d. soggetti 'apicali'), nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio. Non è esclusa, tuttavia, la possibilità che anche le altre funzioni aziendali siano coinvolte, a titolo di concorso ex art. 110 cod. pen., nella commissione del reato. Infine, occorre ricordare che sono considerati Destinatari anche i soggetti di cui all'art. 2639 c.c., ovverosia, coloro che non sono formalmente investiti della funzione ma svolgono di fatto le medesime attività per essa previste, oppure svolgono altra funzione diversamente qualificata ma coincidente nei contenuti.

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 prevenire ed impedire il verificarsi dei reati che ne formano oggetto.

3) PRINCIPALI AREE DI ATTIVITÀ A RISCHIO

Le aree di attività considerate più specificatamente a rischio in relazione ai reati societari sono ritenute le seguenti:

1. redazione del bilancio, della relazione sulla gestione e di altre comunicazioni sociali;
2. operazioni societarie che possano incidere sull'integrità del capitale e/o del patrimonio sociale;
3. le attività soggette a vigilanza di Cdatorità pubbliche in base alla disciplina di settore;
4. informative e rapporti con gli organi di informazione e stampa.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dall'Organo Amministrativo di SILAQ SERVICE S.R.L., anche su proposta dell'ODV, al quale è dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal Codice Etico adottato da SILAQ SERVICE S.R.L. alla cui osservanza sono tenuti tutti i Destinatari.

4) PRINCIPI GENERALI DEI CONTROLLI ESISTENTI

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), i soggetti aziendali coinvolti nella gestione delle aree a rischio individuate in relazione ai reati societari di cui all'art. 25 *ter* del D.Lgs. 231/01 sono tenuti, al fine di prevenire e impedire il verificarsi dei reati, al rispetto di una serie di principi di controllo, basati sull'assunto che la trasparenza e la correttezza contabile si fonda sulla verità, accuratezza e completezza delle informazioni di base per le relative registrazioni contabili.

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

- a) l'agevole registrazione contabile;
- b) l'individuazione dei diversi livelli di responsabilità;
- c) la ricostruzione accurata della operazione, anche al fine di ridurre la probabilità di errori interpretativi.

Il sistema di controllo di SILAQ SERVICE S.R.L. è costituito nelle sue linee generali secondo i principi di controllo generali, di seguito descritti:

- TRACCIABILITA' DELLE OPERAZIONI/ATTI

Ogni operazione o fatto gestionale sensibile e/o rilevante è documentato, coerente e congruo, così che in ogni momento è possibile identificare la responsabilità di chi ha operato (valutato, deciso, Cdatorizzato, effettuato, rilevato nei libri, controllato l'operazione).

- SEGREGAZIONE DELLE FUNZIONI

All'interno di un processo aziendale, funzioni separate decidono un'operazione, l'Cdatorizzano, eseguono operativamente, registrano e controllano. Una contrapposizione tra responsabilità risulta teoricamente opportuna in quanto disincentiva la commissione di errori od irregolarità da parte di una funzione ed eventualmente ne permette l'individuazione da un'altra coinvolta nel processo.

- EVIDENZA FORMALE DEI CONTROLLI

I controlli effettuati all'interno di un processo o una procedura sono adeguatamente formalizzati e documentati, così che si possa, anche in un momento successivo, identificare chi ha eseguito un controllo ed il suo corretto operare.

5) PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare cCdasa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25 *ter* del Decreto);
- porre in essere, collaborare o dare cCdasa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Al fine di garantire il rispetto dei suddetti divieti, ai Destinatari è fatto espresso obbligo di rispettare i principi di comportamento di seguito indicati:

- garantire il rispetto delle regole comportamentali previste nel Codice Etico di SILAQ SERVICE S.R.L., con particolare riguardo all'esigenza di assicurare che ogni operazione e transazione sia correttamente registrata, Cdatorizzata, verificabile, legittima, coerente e congrua;
- tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'esecuzione di tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
- tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni necessarie per consentire di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società;
- garantire il rispetto dei principi di integrità, correttezza e trasparenza così da consentire ai destinatari di pervenire ad un fondato ed informato giudizio sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi;
- osservare le prescrizioni imposte dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo;
- astenersi dal compiere qualsivoglia operazione o iniziativa qualora vi sia una situazione di conflitto di interessi, ovvero qualora sussista, anche per conto di terzi, un interesse in conflitto con quello della Società;
- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale prevista dalla legge, nonché la libera formazione della volontà assembleare;
- astenersi dal porre in essere operazioni simulate o altrimenti frCdadolente, nonché dal diffondere notizie false e/o non corrette e/o fuorvianti, idonee a provocare l'alterazione del prezzo di strumenti finanziari;
- gestire con la massima correttezza e trasparenza il rapporto con le Pubbliche Cdatorità, ivi incluse quelle di Vigilanza;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Cdatorità pubbliche di Vigilanza, non ostacolando l'esercizio delle funzioni di vigilanza da queste intraprese;

- tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione;
- improntare le attività ed i rapporti con le altre Società del Gruppo alla massima correttezza, integrità e trasparenza, così da garantire il rispetto delle leggi e dei regolamenti vigenti.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'Organismo di Vigilanza potrà predisporre controlli dei quali dovrà essere fornita evidenza scritta.

In ogni caso, dovrà tenersi conto, in relazione alle specifiche fattispecie di reato di seguito indicate, delle previsioni di cui al successivo par. 6.

6) PRINCIPI DI ATTUAZIONE DEL MODELLO NELLE ATTIVITA' A RISCHIO

Di seguito sono descritte le modalità di attuazione dei principi sopra richiamati in relazione alle diverse tipologie di reati societari.

6.1) BILANCI ED ALTRE COMUNICAZIONI SOCIALI

Per la prevenzione dei reati relativi alla predisposizione delle comunicazioni indirizzate ai soci e al pubblico in generale, nonché ai fini della formazione del bilancio è necessario che la procedura seguita in azienda garantisca:

- il rispetto dei principi di compilazione dei documenti contabili di cui all'art. 2423 cod. civ.;
- il rispetto del principio di completezza del bilancio, mediante l'indicazione di tutti i dati prescritti dalla normativa vigente (cfr. artt. 2424, 2425 e 2427 cod. civ.);
- l'elencazione dei dati e delle notizie che ciascuna funzione aziendale interessata deve fornire; l'indicazione delle altre funzioni aziendali a cui i dati devono essere trasmessi; i criteri per la loro elaborazione; la tempistica di consegna;
- la trasmissione dei dati alla funzione responsabile per via informatica, affinché resti traccia dei vari passaggi e siano identificabili i soggetti che hanno operato;
- la tempestiva trasmissione all'Organo Amministrativo della bozza di bilancio e della relazione della società di revisione, garantendo l'idonea registrazione di tale trasmissione;
- la giustificazione di ogni eventuale variazione dei criteri di valutazione adottati per la redazione dei documenti contabili sopra richiamati e delle relative modalità di applicazione. Tali situazioni devono, in ogni caso, essere tempestivamente comunicate all'OdV;

- la preventiva approvazione, da parte degli organi aziendali competenti, delle operazioni societarie potenzialmente rilevanti ai fini del Decreto, qualora siano caratterizzate da una discrezionalità di valutazione che possa comportare significativi impatti sotto il profilo patrimoniale o fiscale;
- la tracciabilità delle operazioni che comportino il trasferimento e/o il deferimento di posizioni creditorie.

6.2) TUTELA DEL CAPITALE SOCIALE

Tutte le operazioni sul capitale sociale della Società, di costituzione di società, destinazione di utili e riserve, di acquisto e cessione di partecipazioni o di aziende o loro rami, di fusione, scissione e scorporo, nonché tutte le operazioni potenzialmente idonee a ledere l'integrità del capitale sociale debbono essere realizzate in base a specifiche procedure aziendali all'uopo predisposte.

Queste debbono prevedere:

- l'esplicita approvazione, da parte dell'Organo Amministrativo, di ogni attività relativa alla costituzione di nuove società, all'acquisizione o alienazione di partecipazioni societarie, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni;
- l'espletamento di apposite riunioni con il Sindaco in carico (se presente) e con l'OdV

6.3) ATTIVITA' SOGGETTE A VIGILANZA

La predisposizione delle comunicazioni alle Cdatorità pubbliche di Vigilanza dovrà rispondere ai seguenti criteri:

- dovranno essere individuati i responsabili delle segnalazioni periodiche alle Cdatorità previste o prescritte da leggi e regolamenti;
- dovrà essere data attuazione a tutti gli interventi di natura organizzativa necessari ad assicurare la corretta e completa predisposizione delle comunicazioni ed il loro puntuale invio alle Cdatorità pubbliche di Vigilanza;
- in caso di accertamenti ispettivi da parte delle Cdatorità pubbliche di Vigilanza, dovrà essere fornita adeguata collaborazione da parte delle unità aziendali competenti.

Dovranno, inoltre, essere garantite:

- la tracciabilità del processo relativo alle comunicazioni alle Cdatorità di Vigilanza, da effettuare nel rispetto della normativa vigente (ad es., mediante documentazione degli incontri con i rappresentanti delle Cdatorità);
- l'invio, da parte delle funzioni competenti, di *report* periodici all'Organo Amministrativo, al fine di rendere edotto il vertice aziendale in merito allo stato dei rapporti con le Cdatorità di Vigilanza.

Tutte le comunicazioni trasmesse alle Cdatorità dovranno essere tenute a disposizione dell'Organismo di Vigilanza per le verifiche interne periodiche.

6.4) CONFLITTI DI INTERESSE

In materia di conflitti di interesse, è necessario che la procedura seguita in azienda garantisca la definizione dei casi in cui si potrebbero verificare i conflitti di interesse, prescrivendo e/o indicando:

- la raccolta di una dichiarazione periodica di assenza di conflitti di interesse e del rispetto del Codice Etico dal *management* della Società;
- l'individuazione puntuale dei soggetti che devono presentare tali dichiarazioni;
- le tempistiche e le responsabilità per il monitoraggio delle medesime dichiarazioni;
- i criteri per l'identificazione delle situazioni di potenziale conflitto di interesse;
- le regole comportamentali da seguire in occasione della effettuazione di operazioni straordinarie, ovvero della elaborazione di situazioni economiche, patrimoniali e finanziarie di carattere straordinario.

7) COMPITI DELL'ORGANISMO DI VIGILANZA

I compiti dell'ODV concernenti l'osservanza e l'efficacia del Modello in materia di reati societari sono i seguenti:

a) per quanto riguarda il bilancio e le altre comunicazioni sociali:

- monitoraggio sull'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati di false comunicazioni sociali;
- esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;

b) per quanto riguarda le altre attività a rischio:

- verifiche periodiche sul rispetto delle procedure interne e delle regole di *corporate governance*;
- monitoraggio sull'efficacia delle stesse a prevenire la commissione di reati;
- esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.

L'ODV deve riportare i risultati della propria attività di vigilanza e controllo in materia di reati societari con cadenza periodica annuale alla Direzione di SILAQ SERVICE S.R.L. che, nel caso in cui dagli accertamenti svolti dall'ODV risultasse la violazione di previsioni contenute nella presente Parte speciale, la commissione di un reato o il tentativo di commetterlo, riferirà all'Amministratore per l'adozione dei provvedimenti necessari ed opportuni.

PARTE SPECIALE “C”

REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

INDICE

- 1) LA RESPONSABILITÀ DELL'ENTE IN TEMA DI SALUTE E SICUREZZA SUL LAVORO
- 2) DESCRIZIONE DEI REATI CONTRO LA VITA E L'INCOLUMITÀ INDIVIDUALE CONTEMPLATI NELL'ART. 25 *SEPTIES* DEL DECRETO
 - 2.1) OMICIDIO COLPOSO (ART. 589 C.P.)
 - 2.2) LESIONI COLPOSE (ART. 590 C.P.)
- 3) VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E A TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO
- 4) AREE DI RISCHIO
- 5) DESTINATARI DELLA PARTE SPECIALE
- 6) PRINCIPI GENERALI DI COMPORTAMENTO
- 7) PRINCIPI DI ATTUAZIONE DEL MODELLO NELLE ATTIVITÀ A RISCHIO
- 8) STRUTTURA ORGANIZZATIVA E DELEGHE DI FUNZIONI
- 9) ISTRUZIONI E VERIFICHE DELL'ODV

1. LA RESPONSABILITÀ DELL'ENTE IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO.

L'art. 25-*septies* contempla la responsabilità dell'ente in relazione ai delitti di omicidio colposo e lesioni colpose gravi e gravissime, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il testo originario dell'art. 25-*septies* comminava la sanzione pecuniaria pari a 1000 quote (ovvero non inferiore a 258.000,00 euro, visto che ai sensi dell'art. 10 del medesimo decreto il valore di una quota va da un minimo di 258 ad un massimo di 1.549 euro) e quelle interdittive (che contemplano l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di concessioni ed Cdatorizzazioni, il divieto di contrattare con la pubblica amministrazione, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni o servizi) da tre mesi ad un anno in relazione a tutte le ipotesi di omicidio colposo e lesioni colpose gravi e gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute e sicurezza.

Il D. Lgs. 81/08, recante "*Attuazione dell'art. 1 della legge 2 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*" (di seguito anche T.U. sulla sicurezza), ha rimodulato l'entità delle sanzioni applicabili agli enti in relazione alla gravità delle violazioni contestabili:

- sanzione pecuniaria pari a 1000 quote e sanzioni interdittive per una durata non inferiore a tre mesi e non superiore ad un anno per l'ipotesi di omicidio colposo, commesso con violazione dell'art. 55, comma 2 del T.U. (art. 25-*septies*, comma 1);
- sanzione pecuniaria non inferiore a 250 quote e non superiore a 500 e sanzioni interdittive per una durata non inferiore a tre mesi e non superiore ad un anno nel caso di omicidio colposo commesso con violazione delle norme sulla tutela della sicurezza sul lavoro (art. 25-*septies*, comma 2);
- sanzione pecuniaria in misura non superiore a 250 quote e sanzioni interdittive per una durata non superiore a sei mesi nel caso di lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della sicurezza sul lavoro (art. 25-*septies*, comma 3).

Si precisa che le sanzioni interdittive, che si caratterizzano per l'effetto particolarmente afflittivo che sortiscono sull'attività dell'ente, potranno essere applicate alle aziende anche in via cCdatelare nelle more del giudizio volto ad accertare la responsabilità amministrativa dell'ente.

Stando a quanto previsto dall'art. 55, comma 2 e dalle norme ivi richiamate per effetto di rinvii a catena, le condotte suscettibili di determinare in capo all'ente l'irrogazione delle sanzioni più gravi di cui all'art. 25-*septies*, sono le seguenti:

- a) mancata adozione, da parte del datore di lavoro, del documento di valutazione del rischio di cui all'art. 28 T.U. (adempimento non delegabile ex art. 17, co. 1, lett a);
- b) adozione, da parte del datore di lavoro, del documento di valutazione del rischio ma *in assenza* di alcuni elementi, quali:
 - la relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa (art. 28, co. 2, lett. a);

- l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuati adottati (art. 28, co. 2, lett. b);
 - l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri (art. 28, co. 2, lett. d);
 - l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento (art. 28, co. 2, lett. f);
- c) violazione, da parte del datore di lavoro, delle disposizioni di cui all'art. 18, lett. q) e z) prima parte, secondo cui il datore di lavoro medesimo deve:
- prendere *appropriati* provvedimenti per evitare che le misure tecniche adottate possano cedere rischi per la *salute della popolazione* o *deteriorare l'ambiente* esterno verificando periodicamente la perdurante assenza di rischio;
 - aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro.

Inoltre, sul piano soggettivo, è necessario che le indicate violazioni siano state commesse nell'ambito di imprese rientranti nelle categorie di cui all'art. 31, co. 6, lett. a), b), c), d) ed f):

- quelle di cui all'art. 2 del d.lgs. n. 334/1999 (ove, cioè, sono presenti sostanze pericolose), soggette all'obbligo di notifica o rapporto ai sensi dello stesso T.U. sulla sicurezza;
- centrali termoelettriche;
- impianti ed installazioni di cui al d.lgs. n. 230/1995, attuativo delle direttive Euratom in tema di radiazioni ionizzanti;
- aziende per la fabbricazione ed il deposito di esplosivi, polveri e munizioni;
- industrie estrattive con oltre 50 lavoratori;

ovvero, operanti nei settori di attività richiamati dall'art. 55, co. 2, lett. b) e c):

- aziende in cui si svolgono attività che espongono i lavoratori a rischi biologici di cui all'art. 268, co. 1, lett. c) e d) – ovvero, gli agenti biologici definiti di gruppo 1 o di gruppo 2 – da atmosfere esplosive, cancerogeni mutanti, e da attività di manutenzione, rimozione, smaltimento e bonifica di amianto;
- attività disciplinate dal Titolo IV (e cioè i cantieri temporanei e mobili) caratterizzate dalla compresenza di più imprese e la cui entità presunta di lavoro non sia inferiore a 200 uomini al giorno.

Quindi, laddove la violazione incriminata degli obblighi in delegabili di cui all'art. 55, comma 2 del T.U. sulla sicurezza venga realizzata in un settore operativo diverso da quelli sopra elencati, l'ente potrà comunque essere chiamato a rispondere ai sensi del D. Lgs. 231/01 per i delitti di omicidio colposo e lesioni colpose, ma si applicheranno le più miti sanzioni di cui al 2° o al 3° comma dell'art. 25-septies.

2. DESCRIZIONE DEI REATI CONTRO LA VITA E L'INCOLUMITA' INDIVIDUALE CONTEMPLATI NELL'ART. 25 SEPTIES DEL DECRETO

2.1 OMICIDIO COLPOSO (ART. 589 C.P.)

Il reato si configura quando taluno cagiona involontariamente la morte di una persona per effetto di una condotta consistente nella violazione di norme precdazionali non scritte di diligenza, prudenza e perizia, ovvero nell'inosservanza di misure cCdatelari prescritte da leggi, regolamenti, ordini o discipline.

Le modalità di realizzazione della condotta colposa possono essere sia attive che omissive, purché, in quest'ultimo caso, sussista in capo al soggetto chiamato a rispondere del reato un particolare obbligo giuridico di impedire l'evento morte: è questo il caso dell'imprenditore datore di lavoro, o del soggetto da questi delegato, tenuto per legge alla eliminazione di ogni situazione di pericolo per l'integrità e la salute psico-fisica dei propri lavoratori.

L'art. 589, comma 2, prevede una circostanza aggravante del reato, per l'ipotesi in cui l'evento morte sia conseguenza della violazione della normativa per la prevenzione degli infortuni sul lavoro.

2.2. LESIONI COLPOSE (ART. 590 C.P.)

Il reato si configura nel fatto di chi cagiona colposamente in altri una malattia nel corpo o nella mente. Non è richiesto, quale elemento costitutivo indefettibile, l'uso della violenza. E' sufficiente qualsiasi condotta idonea a cagionare una qualsiasi alterazione, anatomica o funzionale dell'organismo, ancorché localizzata e non influente sulle condizioni organiche generali.

La lesione può essere

- 1) **lieve** se deriva una malattia o una incapacità di attendere alle ordinarie occupazioni – per tale intendendosi non la sola attività lavorativa – non superiore a 40 giorni;
- 2) **grave** se dal fatto deriva:
 - una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
 - l'indebolimento permanente di un senso o di un organo.
- 3) **gravissima** se il fatto produce:
 - una malattia certamente o probabilmente insanabile;
 - la perdita di un senso;

- la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;
- la deformazione, ovvero lo sfregio permanente del viso.

Il nuovo art. 25 *septies* del D. Lgs. 231/01 limita la propria operatività alle ipotesi aggravate di cui al III comma dell'art. 590 c.p., e cioè alle ipotesi di lesione grave o gravissima cagionate dalla violazione delle norme per la prevenzione degli infortuni sul lavoro. Quindi, in considerazione di tale rinvio, la responsabilità dell'ente andrà esclusa nei casi in cui la violazione della normativa antinfortunistica determini solo una lesione lieve, mentre andrà senz'altro affermata ove la lesione grave o gravissima sia determinata dalla violazione di norme poste a tutela dell'igiene e della salute sul lavoro, ovvero quelle specificamente dettate per prevenire le malattie professionali.

3. VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E A TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

Ai fini della responsabilità amministrativa degli enti, la nuova previsione di cui all'art. 25 *septies* attribuisce rilievo non solo alla violazione della normativa antinfortunistica, bensì anche a quella posta a tutela dell'igiene e della salute sul lavoro.

Si precisa che:

- Il **dovere di igiene, salute e sicurezza sul lavoro** si realizza o attraverso l'attuazione di misure specifiche imposte tassativamente dalla legge o, in mancanza, con l'adozione dei mezzi idonei a prevenire ed evitare sinistri e, in genere, lesioni alla salute psicofisica dei lavoratori, assunti con i sussidi dei dati di comune esperienza, prudenza, diligenza, prevedibilità, in relazione all'attività svolta.
L'art. 2087 c.c., in forza del quale *«l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro»* ha carattere generale e sussidiario, di integrazione della specifica normativa posta a presidio del diritto ad un ambiente di lavoro salubre e sicuro.
Pertanto, sono da rispettare non soltanto le specifiche norme contenute nelle leggi speciali a garanzia degli interessi suddetti, ma anche quelle che, se pure stabilite da leggi generali, sono ugualmente dirette a prevenire gli infortuni stessi, come l'art. 437 c.p. che sanziona l'omissione di impianti o di segnali destinati a tale scopo.
- La legislazione speciale, anche quando fa riferimento a situazioni definite come **“luoghi di lavoro”**, **“posti di lavoro”**, ecc., richiede che la misura preventiva riguardi l'intero ambiente in cui si svolge l'attività lavorativa. L'ambiente di lavoro, pertanto, deve essere reso sicuro in tutti i luoghi nei quali chi

è chiamato ad operare possa comunque accedere, per qualsiasi motivo, anche indipendentemente da esigenze strettamente connesse allo svolgimento delle mansioni disimpegnate.

- Per la ravvisabilità della circostanza del fatto commesso con violazione delle norme per la prevenzione degli infortuni e la tutela della salubrità dell'ambiente di lavoro è necessario che sussista **legame cCdasale**, secondo i principi di cui agli artt. 40 e 41 c.p., tra siffatta violazione e l'evento dannoso. Dunque è necessario che l'evento lesivo rappresenti la traduzione di uno dei rischi specifici che la norma violata mirava a prevenire.
- Poiché la normativa antinfortunistica mira a salvaguardare l'incolumità del lavoratore non soltanto dai rischi derivanti da accidenti o fatalità, ma anche da quelli che possono scaturire da sue stesse avventatezze, negligenze e disattenzioni, purché normalmente connesse all'attività lavorativa, la responsabilità del datore di lavoro può essere esclusa, per cCdasale sopravvenuta solo in presenza di un **comportamento del lavoratore** abnorme ed esorbitante rispetto al procedimento lavorativo ed alle precise direttive organizzative ricevute. Tuttavia, in caso d'infortunio sul lavoro originato dall'assenza o dall'inidoneità delle misure di prevenzione, nessuna efficienza cCdasale può essere attribuita ai comportamenti – non solo disaccorti o maldestri, ma anche del tutto imprevedibili ed opinabili – del lavoratore infortunato che abbiano dato occasione all'evento, quando questo sia da ricondursi alla mancanza di quelle cCdatele che, se adottate, sarebbero valse a neutralizzare anche il rischio di siffatti comportamenti.
- **Soggetti passivi** del reato: le norme in materia di igiene, salute e sicurezza sul lavoro sono poste a tutela non solo dei lavoratori dipendenti, ma di chiunque in un modo o nell'altro possa essere esposto a pericolo dallo svolgimento dell'attività imprenditoriale nel cui ambito le norme stesse spiegano validità ed efficacia. Ne consegue che, ove un infortunio si verifichi per inosservanza degli obblighi di sicurezza e di salubrità dell'ambiente normativamente imposti, tale inosservanza non potrà non far carico, a titolo di colpa *ex art. 43 c.p.*, su chi detti obblighi avrebbe dovuto rispettare, e quindi sulla società, poco importando che ad infortunarsi sia stato un lavoratore subordinato, un soggetto a questi equiparato o, addirittura, una persona estranea all'ambito imprenditoriale, purché sia ravvisabile il nesso cCdasale con l'accertata violazione.

4. AREE DI RISCHIO

Rispetto ai reati sopra descritti, la predisposizione di idonee misure di prevenzione deve riguardare:

- A. la presenza di operatori interni ed esterni, e più in generale di persone fisiche, nei luoghi di lavoro e nelle aree circostanti.
- B. lo svolgimento di qualunque attività di lavoro che, non presupponendo una Cdatonomia gestionale, sia finalizzata a fornire un servizio completo e ben individuabile.

Nell'ambito di SILAQ SERVICE S.R.L. il rischio di verifica dell'evento morte o di una lesione grave o gravissima all'integrità individuale del lavoratore o del terzo è estremamente limitato ma può astrattamente conseguire:

1. dalla presenza del soggetto nei luoghi in cui si svolge l'attività (ad es. inalazioni di polveri e vapori, caduta di oggetti e materiali inerti dagli scaffali o da apparecchiature in movimento, esposizioni a rumori oltre soglia, condizioni microclimatiche sfavorevoli, intrinseca pericolosità dello stato dei luoghi);
2. all'organizzazione logistica degli orari e dei ritmi di lavoro (ad es. stress psicofisico causato da orari e ritmi di lavoro eccessivo; disturbi acuti e cronici per posizioni di lavoro in piedi o per posture incongrue);
3. ai fattori di pericolo connessi alle attività lavorative (ad es. uso del videoterminale, posture incongrue, esposizione a sostanze chimiche pericolose classificate come molto tossiche, tossiche, nocive, sensibilizzanti, irritanti, esposizione ad agenti biologici, proiezione di polveri e materiali in genere sugli occhi);
4. allo svolgimento delle specifiche mansioni di impiegato od altre;
5. alle specifiche mansioni comportanti lo svolgimento dell'attività lavorativa, in tutto o in parte, al di fuori dei luoghi di lavoro aziendali (ad es. rischi connessi agli spostamenti ed ai viaggi per ragioni di lavoro, con particolare riferimento all'attività di Tecnico Consulente o Consulente Commerciale).

In particolare, si qualificano come **rischi prevalenti**:

- caduta di materiale dall'alto;
- ribaltamento e crollo e cedimento di strutture o solai in genere;
- scavi e seppellimento;
- abrasioni, tagli e schiacciamenti di parti del corpo;
- contusioni e dolori alla schiena e ad altre parti del corpo;
- urti con il capo e/o con altre parti del corpo contro oggetti sporgenti;
- rischi di folgorazioni e derivanti dalla presenza di impianti elettrici;
- incendio ed esplosione per impiego e deposito di materiali infiammabili e altri agenti chimici,
- rischi derivanti da potenziali atmosfere esplosive;

Si qualificano come **rischi concorrenti** (atti ad aggravare i rischi prevalenti di cui sopra):

- carenze strutturali dell'ambiente di lavoro;
- altezza ambienti;
- piani di lavoro e/o superfici scivolose e ingombrate da materiale con rischio di inciampo e caduta di persone;

- illuminazione, fenomeni di abbagliamento (sole, zone d'ombra, ecc), scarsa visibilità, colpo di calore o di sole, effetti da basse temperature, presenza del vento e/o della pioggia;

Altri rischi potranno essere identificati e comportare un aggiornamento del Documento di Valutazione del Rischio (DVR) e, conseguentemente, della presente Parte Speciale di cui il predetto documento è parte integrante.

5. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono gli amministratori, i direttori generali o *managers*, i delegati alla sicurezza ed alla tutela dell'igiene e della salute nei luoghi di lavoro, i dirigenti, i preposti, tutti i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività di rischio, nonché tutti coloro che, operando a qualsiasi titolo in tali aree, possono comunque, direttamente o indirettamente, commettere o agevolare la commissione dei reati sopra indicati.

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 dei reati previsti nel Decreto.

Sono, tuttavia, destinatari di specifici compiti le figure di seguito descritte:

- **Datore di lavoro:** il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa
- **Dirigente:** persona che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa;
- **Preposto:** persona che, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende alla attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa
- **Lavoratore:** persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. I lavoratori possono essere riconosciuti responsabili, esclusivi

o concorrenti, degli infortuni o degli incidenti che si verificano nei luoghi di lavoro soltanto se i datori di lavoro, i dirigenti e i preposti abbiano ottemperato a tutti gli obblighi che su di loro ricadono e il lavoratore abbia posto in essere una condotta “abnorme” e cioè:

- dolosa;
- frutto di rischio elettivo;
- anormale e atipica e, quindi, non prevedibile;
- eccezionale e incompatibile con il sistema di lavorazione;
- di deliberata inosservanza dei dispositivi antinfortunistici, d’istruzioni o compiti esecutivi (ad esempio il lavoratore continua a non indossare i DPI dopo aver ricevuto opportuna formazione e dopo essere stato richiamato sia dal preposto sia dai dirigenti).

6. PRINCIPI GENERALI DI COMPORTAMENTO

Ai fini della prevenzione dei reati di cui all’art. 25 *septies* del Decreto, in conformità alle disposizioni dell’art. 30 del D. Lgs. n. 81/2008, il Modello prevede l’espreso divieto a carico dei destinatari di:

- porre in essere o concorrere in qualsiasi forma nella realizzazione di comportamenti tali da integrare le fattispecie di reato considerate;
- porre in essere o concorrere in qualsiasi forma nella realizzazione di comportamenti che, sebbene siano tali da non integrare i reati indicati, possano potenzialmente tradursi in essi o agevolarne la commissione.

Più specificamente, la presente Parte Speciale impone, in capo a tutti i Destinatari, l’espreso obbligo di:

- a) osservare rigorosamente tutte le norme di legge e di regolamento in materia di igiene, salute e sicurezza nell’ambiente di lavoro;
- b) agire sempre nel rispetto dei protocolli e delle procedure aziendali interne che su tali norme si fondano;
- c) astenersi dal porre in essere qualsiasi comportamento che sia di ostacolo all’attuazione di una adeguata attività di prevenzione e protezione dai rischi professionali, come occultare dati od omettere informazioni rilevanti per l’accertamento delle aree di rischio;
- d) assicurare in tutti i luoghi di lavoro un controllo continuo, capillare e diffuso circa il rispetto delle norme antinfortunistiche da parte di chiunque possa accedervi.
- e) predisporre e garantire, nell’ipotesi di acquisto di macchinari da montarsi in loco, le condizioni di sicurezza del lavoro di installazione;
- f) aggiornarsi ed aprirsi alle nuove acquisizioni tecnologiche;
- g) nel caso che uno o più dispositivi di sicurezza di un macchinario si rivelino in concreto insufficienti, predisporre tutti gli accorgimenti ulteriori, rispetto ai dispositivi già esistenti o indicati dalla legge

antifortunistica, che rendano il funzionamento del macchinario assolutamente sicuro per gli operatori che vi lavorano;

- h) destinare all'esecuzione di ogni attività lavorativa, tenuto conto della natura, dell'oggetto, delle particolarità e dei margini di rischio, persone di collaudata esperienza o che siano senza riserve all'altezza della stessa;
- i) in presenza di fattori che possano compromettere la felice realizzazione del lavoro (come ad es. l'ora notturna), affidarne l'esecuzione ad un numero di addetti qualificati tale da consentire di superare agevolmente gli eventuali disagi;
- j) gestire gli utensili, gli attrezzi, i materiali o i prodotti necessari all'esecuzione del lavoro, potenzialmente fonte di pericolo, in modo tale da evitare che possano essere usati impropriamente da altre persone;
- k) mantenere e seguire i percorsi appositamente predisposti, evitando assolutamente di ingombrarli con materiali o attrezzature;
- l) utilizzare la corrente elettrica per l'alimentazione di attrezzi e/o utensili nel rispetto delle norme di legge e di buona tecnica, assicurando il buono stato di quadri elettrici, prese spine e prolunghe, che devono essere correttamente installate e posizionate;
- m) rispettare i cartelli segnalatori e indicatori esposti nella azienda;
- n) ridurre la ripetitività delle azioni, agevolare l'alternanza delle esposizioni a freddo, caldo, radiazioni UV ed a microclimi particolarmente insalubri;

Nell'ambito dei predetti codici comportamentali sono:

Obblighi specifici del preposto:

- affidare i compiti ai lavoratori tenendo conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;
- adottare le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni possano accedere alle zone che li espongono ad un rischio grave e specifico;
- adottare le misure per il controllo delle situazioni di rischio in caso d'emergenza e dare le opportune e necessarie istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- astenersi dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
- esigere e vigilare sull'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e d'igiene sul lavoro oltre all'uso dei mezzi di protezione individuali;

- verificare costantemente l'adempimento dell'obbligo di organizzazione del coordinamento e della reciproca informazione fra le imprese presenti in cantiere.

Obblighi dei lavoratori:

- preservare la salute e la sicurezza proprie e delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni ed omissioni, conformemente alla formazione, alle istruzioni e ai mezzi forniti loro dal Datore di Lavoro;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva e individuale;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze e i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- segnalare immediatamente al preposto, al dirigente o al Datore di Lavoro secondo le rispettive attribuzioni, le deficienze di mezzi e dispositivi, nonché altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso d'urgenza e compatibilmente alle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli; in caso di inerzia da parte dei soggetti di cui sopra darne notizia al Rappresentante dei Lavoratori per la Sicurezza nonché all'OdV;
- non rimuovere o modificare senza Cdatorizzazione i dispositivi di sicurezza, di segnalazione e di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di propria competenza o che, comunque, possano compromettere la sicurezza propria o di altri;
- sottoporsi ai controlli sanitari previsti dalla legge e dal protocollo sanitario interno;
- contribuire, insieme al Datore di Lavoro, ai dirigenti e ai preposti, all'adempimento di tutti gli obblighi imposti dall'Cdatorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

7. PRINCIPI DI ATTUAZIONE DEL MODELLO NELLE ATTIVITA' A RISCHIO

Ai fini del rispetto dei principi sopra indicati, il Documento di Valutazione dei Rischi (al cui contenuto si rinvia):

- Individua le misure di prevenzione e di protezione e i relativi dispositivi di protezione individuale;
- Prevede un programma di miglioramento in relazione alla valutazione dei rischi per la sicurezza e la salute durante il lavoro.

8. STRUTTURA ORGANIZZATIVA E DELEGA DI FUNZIONI

L'adempimento degli obblighi imposti al datore di lavoro in materia di igiene, salute e sicurezza sul lavoro, ad esclusione del residuo non delegabile espressamente previsto dalla legge, può essere delegato ad uno o più responsabili all'uopo individuati.

Ai fini della validità e dell'effettività della delega occorre che siano rispettate le seguenti condizioni (art. 16 d.lgs n. 81/2008):

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

Alla delega è data adeguata e tempestiva pubblicità. La delega di funzioni non esclude l'obbligo di vigilanza in capo al datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. La vigilanza si esplica anche attraverso i sistemi di verifica e controllo di cui all'articolo 30, comma 4, d.lgs. n. 81/2008.

Nell'ambito di SILAQ SERVICE S.R.L. il Datore di lavoro è il Rag. Gabriele Alberti, il Responsabile del servizio prevenzione e protezione è il Sig. Flavio Rinaldi ed il Responsabile dei Lavoratori per la Sicurezza è il Sig. Tiziano Marzocchi ed il Medico del Lavoro è il Dott. Luca Berrinzi.

9. ISTRUZIONI E VERIFICHE DELL'ODV

Con periodicità almeno semestrale l'ODV, con almeno due dei suoi membri, esegue sopralluoghi nelle varie aree di rischio sopra riportate, al fine di verificare l'effettiva attuazione delle disposizioni contenute nella presente Parte Speciale.

Tali operazioni possono essere svolte anche durante visite ispettive (ad es. qualità) già organizzate con altri fini. Ad esse devono partecipare almeno due membri dell'ODV.

L'attività di ispezione si attua mediante la predisposizione di verbale (su carta e/o su supporto informatico) nel quale devono essere indicate:

1. le inadempienze riscontrate;
2. le prescrizioni operative;
3. la necessità di procedere ad eventuali miglioramenti organizzativi e gestionali, ivi compresi l'aggiornamento del DVR e la redazione di ulteriori procedure di sicurezza;
4. eventuali fattori di rischio sopravvenuti e le misure di prevenzione e protezione da adottare per scongiurarne la realizzazione.

In base all'esito del sopralluogo, è comunque in potere dell'ODV ritenere non necessario l'inserimento di una o più delle voci su indicate.

A prescindere e indipendentemente dagli interventi di iniziativa dell'ODV, i preposti, i dirigenti e il Datore di lavoro, in relazione ai rispettivi settori di competenza, devono informare l'ODV, tramite apposite segnalazioni, circa la verifica di infortuni sul lavoro e l'instaurazione di situazioni di rischio sopravvenute nell'ambito delle funzioni che ad essi fanno capo, nonché le iniziative e gli adempimenti eventualmente adottati al fine di scongiurare la realizzazione dei rischi medesimi.

E' sulla base delle suddette attività di ispezione e segnalazione che l'ODV:

- a) verifica costantemente la completezza e l'efficacia delle disposizioni della presente Parte Speciale;
- b) cura l'emanazione e l'aggiornamento delle procedure aziendali e dei protocolli relativi, delle istruzioni relative agli atteggiamenti da assumere nell'ambito delle attività a rischio, delle forme e delle modalità di svolgimento delle attività ispettive e di segnalazione;
- c) verifica periodicamente – con il supporto delle altre funzioni aziendali competenti – il sistema di deleghe in vigore, segnalando al Consiglio di Amministrazione le modifiche che si rendessero opportune o necessarie ai fini della stessa validità ed efficacia della delega;
- d) verifica periodicamente – con il supporto delle altre funzioni aziendali competenti – la validità di eventuali clCdasole standard finalizzate:
 - all'osservanza da parte di Collaboratori esterni e Partner delle disposizioni del Modello organizzativo e del Codice Etico adottati da SILAQ SERVICE S.R.L.;
 - alla possibilità di SILAQ SERVICE S.R.L. di effettuare efficaci azioni di controllo nei confronti di tutti i Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
 - all'attuazione di meccanismi sanzionatori (ad es. il recesso dal contratto nei riguardi di Partner o di Collaboratori esterni qualora di accertino violazioni delle prescrizioni);
- e) indicare alle funzioni competenti le eventuali integrazioni ai sistemi di gestione aziendale già presenti in SILAQ SERVICE S.R.L.;
- f) accertare ogni eventuale violazione della presente Parte Speciale e/o proporre eventuali sanzioni disciplinari.

PARTE SPECIALE “D”

REATI CONTRO IL PATRIMONIO EX ART. 25-OCTIES

INDICE

1. Le tipologie dei reati contro il patrimonio di cui all’art. 25-octies e i principi di comportamento
 - 1.1 Premessa
 - 1.2 Ricettazione (art. 648 c.p.),
 - 1.3 Riciclaggio (art. 648-bis c.p.)
 - 1.4. Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-ter c.p.)
 - 1.5. Aree aziendali a rischio
 - 1.6. Principi adottati da SILAQ SERVICE S.R.L.
 - 1.7. Istruzioni e verifiche dell’Odv

1. Le tipologie dei reati contro il patrimonio di cui all'art. 25-octies e i principi di comportamento

1.1 Premessa

Con l'attuazione da parte del Governo della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca le misure di esecuzione, è stato introdotto nella disciplina di cui al D.lgs 231/2001 l'art. 25-octies che prevede la responsabilità della società per i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

I reati di riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita erano già rilevanti ai fini del Decreto ma esclusivamente se realizzati transnazionalmente. A seguito dell'introduzione dell'art. 25-octies, i predetti reati, unitamente alla ricettazione, divengono rilevanti anche su base nazionale.

1.2 Ricettazione (art. 648 c.p.)

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

La pena è della reclusione sino a sei anni e della multa sino a 516 euro, se il fatto è di particolare tenuità.

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

Fattispecie

Il reato presuppone l'esistenza di un delitto anteriore che non deve necessariamente essere stato accertato con sentenza irrevocabile né devono essere stati individuati gli Autori, essendo sufficiente che la sua sussistenza risulti dagli atti processuali.

Sotto il profilo oggettivo la condotta criminosa può concretarsi nell'acquisto, nella ricezione e nell'occultamento di cose o denaro proveniente da delitto oppure nell'intromissione finalizzata all'acquisto, alla ricezione o all'occultamento degli stessi beni.

Per la configurabilità della ricettazione è necessaria la consapevolezza della provenienza illecita del bene ricevuto senza che sia necessario conoscere le circostanze di tempo, di modo e di luogo del reato presupposto. Quanto all'elemento del profitto, la cui presenza connota la ricettazione come reato a dolo specifico, è sufficiente qualsiasi utilità o vantaggio derivante dal possesso della cosa, né si esige che l'agente abbia effettivamente conseguito il profitto avuto di mira.

1.3 Riciclaggio (art. 648-bis c.p.)

Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.

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

La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

Si applica l'ultimo comma dell'art. 648.

Fattispecie

Sotto il profilo dei soggetti attivi, il riciclaggio è reato comune, potendo essere commesso da chiunque. Il reato di riciclaggio si distingue dalle ipotesi di concorso nel reato sulla base di un criterio di carattere temporale (avente, però, solo valore indicativo), per cui si configurerà il concorso quando l'accordo per riciclare i proventi illeciti sia intervenuto prima della commissione del fatto e, viceversa, si configurerà il reato di riciclaggio nell'ipotesi in cui l'accordo intervenga successivamente alla commissione del delitto dal quale provengono i proventi illeciti.

La condotta tipica del reato di riciclaggio presenta una triplice modalità di commissione, ossia la sostituzione, il trasferimento (di beni o utilità) ovvero il compimento di qualsiasi altra operazione tale da ostacolare l'identificazione della provenienza delittuosa dei beni o utilità. Elemento comune delle tre tipologie di condotta consiste nell'ideoneità delle stesse a cedere il verificarsi di un ostacolo all'identificazione di cui sopra, e non la semplice finalità di intralcio, circostanza che costituisce l'evento del reato.

Oggetto della sostituzione o del trasferimento possono essere "denaro, beni o altre utilità" che provengano da un precedente reato non colposo, circostanza che costituisce, di fatto, il presupposto materiale della fattispecie di reato in esame. Per quanto attiene all'elemento soggettivo, il riciclaggio è reato doloso e presuppone, pertanto, la volontaria esecuzione di una delle operazioni tipiche con la consapevolezza della (generica) provenienza del bene riciclato. Ai fini della consumazione del delitto è necessario che alla condotta di sostituzione, trasferimento o altre operazioni di "travestimento" consegua il verificarsi di un effettivo occultamento della provenienza illecita.

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

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.

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

La pena è diminuita nell'ipotesi di cui al secondo comma dell'art. 648.

Si applica l'ultimo comma dell'art. 648

Fattispecie

La fattispecie assicura, nella repressione delle operazioni di riciclaggio, una forma di tutela anche nella fase finale delle operazioni di *recycling*, ossia l'integrazione del denaro di provenienza illecita nei circuiti economici attuata proprio attraverso l'immissione nelle strutture dell'economia legale dei capitali così preventivamente ripuliti. La norma, che interessa, pertanto, la fase del collocamento di proventi illeciti già "lavati", ha, peraltro, un ambito di applicabilità piuttosto limitato, stante la triplice modalità di sussidiarietà, contenuta nella disposizione stessa, rispetto al concorso nel reato base nonché alle disposizioni di cui agli artt. 648 e 648-bis del c.p.

La condotta tipica è incentrata sul concetto di "impiego in attività economiche o finanziarie" che si presta ad interpretazioni più o meno restrittive; la dottrina prevalente adotta, in proposito, un'interpretazione piuttosto restrittiva identificando il concetto con quello di investimento – intrinsecamente caratterizzato da uno scopo di profitto – in attività che non costituiscono operazioni di carattere occasionale o sporadico. L'impiego di capitali illeciti è reato doloso e presuppone, pertanto, la consapevolezza della provenienza delittuosa dei beni.

1.5. Aree aziendali a rischio

La Direzione Amministrazione e Finanza riguardo alla gestione dei flussi finanziari di entrata e di spesa. I singoli dipartimenti in cui è organizzata la struttura societaria (cfr. organigramma allegato alla Parte Generale) relativamente alla selezione e gestione dei fornitori.

Considerazioni applicative

Il rischio di verifica dei suddetti reati (delitti) è considerato minimo alla luce delle considerazioni metodologiche della parte generale.

In particolare occorre osservare come nella storia di SILAQ SERVICE S.R.L. non si ravvisino episodi di coinvolgimenti di dipendenti per i reati ex artt. 648 c.p. , 648 bis c.p. e 648 ter c.p. posti in essere nell'interesse della società ovvero a suo vantaggio.

Si ritiene che in relazione alla assoluta modestia del rischio rilevato, possa essere individuata quale efficace e sufficiente misura di prevenzione l'osservanza dei principi e delle disposizioni adottate dal Codice Etico, la stretta osservanza delle regole dettate dalle Procedure aziendali sotto riportate unitamente alla rigorosa applicazione da parte di SILAQ SERVICE S.R.L. del sistema disciplinare.

1.6. Principi adottati da SILAQ SERVICE S.R.L.

Con riferimento alla categoria dei reati previsti dall'art. 25 *octies*, SILAQ SERVICE S.R.L., nell'espletamento della propria attività, ha adottato una serie di principi e procedure che devono essere osservati da tutti i Destinatari del presente Modello:

- i Principi contenuti nel Codice Etico;
- i Principi dei Rapporti con la Pubblica Amministrazione;
- tutte le attività e le operazioni devono essere improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- devono essere rispettate le procedure aziendali, in materia di gestione ed impiego delle risorse e dei beni aziendali;
- devono essere rispettate le procedure sulle modalità di pagamento;
- deve essere rispettata ogni procedura impartita da SILAQ SERVICE S.R.L. per la gestione di flussi finanziari aziendali;
- devono essere rispettate le procedure per la gestione degli acquisti e delle vendite;
- deve essere rispettata ed osservata ogni procedura prevista a livello aziendale richiamata dal presente Modello ed in quanto tale da considerarsi parte integrante del medesimo.

1.7. Istruzioni e verifiche dell'OdV

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati contro la Personalità Individuale sono i seguenti:

- proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- svolgere verifiche periodiche sul rispetto delle procedure interne e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati;
- esaminare eventuali segnalazioni specifiche ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

PARTE SPECIALE “E”

REATI INFORMATICI

INDICE

PARTE SPECIALE

I REATI INFORMATICI

1. I reati informatici richiamati dall'articolo 24 *bis* del D.Lgs. 231/2001.
- 1.2 Documenti informatici (art. 491-*bis* cod. penale).
- 1.3 Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* cod. penale)
- 1.4 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* cod. penale)
- 1.5 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* cod. penale)
- 1.6 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* cod. penale)
- 1.7 Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. penale)
- 1.8 Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* cod. penale)
- 1.9 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-*ter* cod. penale)
- 1.10 Danneggiamento di sistemi informatici e telematici (art. 635-*quater* cod. penale)
- 1.11 Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-*quinquies*. cod. penale)
- 1.12 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* cod. penale)
2. Funzione della Parte Speciale –Reati Informatici-
3. Principi di riferimento generali
 - 3.1 Il sistema organizzativo in generale
 - 3.2 Principi generali di comportamento
4. Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001
5. Principi generali di controllo
- 6 Principi di riferimento specifici relativi alla regolamentazione delle singole Attività Sensibili
 - 6.1 Gestione e monitoraggio degli accessi ai sistemi informatici e telematici
- 7 I controlli dell'Organismo di Vigilanza

I REATI INFORMATICI

1. I reati informatici richiamati dall'articolo 24 *bis* del D.Lgs. 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.Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di organizzazione, gestione e controllo previsto dal decreto.

A tal fine, si riporta di seguito una descrizione dei reati richiamati dall'art. 24-*bis* del D.Lgs. 231/2001, in base al quale:

- “1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*
- 2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*
- 3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*
- 4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)”.*

1.2 Documenti informatici (art. 491-*bis* cod. penale).

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

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

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

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

- Falsità materiale commessa dal pubblico ufficiale in certificati o Cdatorizzazioni amministrative (art. 477 c.p.):

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

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

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

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

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

- Falsità ideologica commessa dal pubblico ufficiale in certificati o Cdatorizzazioni amministrative (art. 480 c.p.):

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

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

“Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00.

Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro?”;

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

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

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

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

- Falsità in registri e notificazioni (art. 484 c.p.): *“Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Cdatorità di pubblica sicurezza, o a fare notificazioni all'Cdatorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a €*

309,00?”;

- Falsità in scrittura privata (art. 485 c.p.): *“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata”*;

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

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

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

“Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o Cdatorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480”;

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

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

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

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

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

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

- Copie Cdautentiche che tengono luogo degli originali mancanti (art. 492 c.p.):

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

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

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

1.3 Accesso abusivo a un sistema informatico o telematico (art. 615-ter cod. penale):

“Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio”.

1.4 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* cod. penale):

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

1.5 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinqüies* cod. penale):

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

1.6 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* cod. penale):

“Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

- 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- 3) da chi esercita anche abusivamente la professione di investigatore privato”.

1.7 Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. penale):

“Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.”

1.8 Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* cod. penale):

“Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al numero 1 del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.”

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

“Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione, o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore di sistema, la pena è Cdamentata.”

1.10 Danneggiamento di sistemi informatici e telematici (art. 635-*quater* cod. penale):

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

1.11 Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635- *quinquies* cod. penale):

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

1.12 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* cod. penale):

“Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00”.

2. Funzione della Parte Speciale –Reati Informatici.

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, dai Dipendenti, nonché dai Consulenti, come meglio definiti nella parte generale, coinvolti nelle fattispecie di Attività Sensibili.

Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente. Nella parte generale sono stati richiamati i principi ispiratori della normativa e i presidi principali per l’attuazione delle vigenti disposizioni in materia.

Sulla base delle logiche organizzative della SILAQ SERVICE S.R.L., la stessa, con l’adozione e attuazione del Modello persegue l’obiettivo di identificare procedure da riverberare sullo staff della SILAQ SERVICE S.R.L. medesima, in un’ottica di razionalizzazione, economia di scala e ottimizzazione delle attività di monitoraggio e controllo.

In questa parte speciale sono individuati i principi di riferimento per la costruzione del Modello, specificamente previsti in relazione alle fattispecie di Attività Sensibili individuate al fine di prevenire la commissione dei reati informatici.

3. Principi di riferimento generali.

3.1 Il sistema organizzativo in generale

SILAQ SERVICE S.R.L. considera essenziale allo svolgimento della sua attività la promozione e il mantenimento di un adeguato sistema di controllo interno da intendersi come insieme di tutti gli strumenti necessari o utili a indirizzare, gestire e verificare le attività di impresa con l’obiettivo di assicurare il rispetto delle leggi e delle procedure aziendali, di proteggere i beni aziendali, di gestire in modo ottimale ed efficiente le attività.

La responsabilità di realizzare un sistema di controllo efficace è comune a ogni livello della struttura organizzativa di SILAQ SERVICE S.R.L.; di conseguenza, tutti coloro che svolgono la propria attività per SILAQ SERVICE S.R.L., nell'ambito delle funzioni e responsabilità ricoperte, sono impegnati nel definire e nel partecipare attivamente al corretto funzionamento del sistema di controllo interno.

Ciò posto, con specifico riguardo alle problematiche connesse al rischio informatico SILAQ SERVICE S.R.L., conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e (ii) la garanzia della massima continuità del servizio.

3.2 Principi generali di comportamento

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione Cdatorizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che SILAQ SERVICE S.R.L. si pone sono i seguenti:

- **Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti Cdatorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono Cdatorizzati a conoscerla;
- **Integrità:** garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non Cdatorizzati;
- **Disponibilità:** garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'esplicito divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di SILAQ SERVICE S.R.L. rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche cCdasole contrattuali) di:

- porre in essere, collaborare o dare cCdasole alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-*bis* del D.Lgs. 231/2001);

- violare i principi e le procedure aziendali previste nella presente parte speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;
5. evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);

7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa Cdatorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
12. astenersi dall'effettuare copie non specificamente Cdatorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte Cdatorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

4. Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall'art. 24- *bis* del D.Lgs. 231/2001, sono le seguenti:

Gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di Cdautenticazione
- gestione e protezione della postazione di lavoro
- gestione degli accessi verso l'esterno
- gestione e protezione delle reti
- gestione degli output di sistema e dei dispositivi di memorizzazione
- Sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.)

5. Principi generali di controllo

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- **Segregazione delle attività:** si richiede l'applicazione del principio di separazione delle attività tra chi Cdatorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di (i) gestione di un processo e di controllo dello stesso, (ii) progettazione ed esercizio, (iii) acquisto di beni e risorse e relativa contabilizzazione.

- **Esistenza di procedure/norme/circolari:** devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri Cdatorizzativi e di firma:** i poteri Cdatorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della SILAQ SERVICE S.R.L.
- **Tracciabilità:** ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, Cdatorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

6. Principi di riferimento specifici relativi alla regolamentazione delle singole Attività Sensibili

Ai fini dell'attuazione delle regole elencate al precedente capitolo 3, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui al paragrafo 5, nel disciplinare la fattispecie di attività sensibile di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

6.1 Gestione e monitoraggio degli accessi ai sistemi informatici e telematici:

- 1) Esistenza di una normativa aziendale relativa alla gestione del rischio informatico che individui le seguenti fasi:
 - identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;
 - individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
 - individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
 - identificazione delle possibili contromisure;
 - effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure;
 - definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
 - documentazione e accettazione del rischio residuo.
- 2) Esistenza di una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:
 - definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
 - costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;

- puntuale pianificazione delle attività di sicurezza informatica;
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.

3) Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.

4) Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.

5) Attuazione di un sistema di protezione idoneo a identificare e Cdatenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'Cdautenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti Cdautorizzati.

6) Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichino attraverso la verifica e la gestione dei diritti d'accesso.

7) Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.

8) Proceduralizzazione e espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.

9) Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).

10) Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti.

11) Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di *networking*.

12) Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni).

13) Predisposizione e attuazione di una policy aziendale che stabilisce (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.

7. I controlli dell'Organismo di Vigilanza

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili.

Di detti controlli l'Organismo di Vigilanza riferisce all'Organo Amministrativo ed al Collegio Sindacale (se presente), secondo le modalità previste nella Parte Generale del presente Modello.

PARTE SPECIALE “F”

IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE (art. 25- *duodecies* D.Lgs. 231/2001)

INDICE

1. DESTINATARI DELLA PARTE SPECIALE E
2. I DELITTI INERENTI ALL'IMPIEGO DI LAVORATORI IRREGOLARI
 - 2.1. CONSIDERAZIONI SUL REATO DI CAPORALATO
 - 2.2. CONSIDERAZIONI SULLA RESPONSABILITA' SOLIDALE NEGLI APPALTI
3. PROCESSI SENSIBILI
4. PRINCIPI DI RIFERIMENTO GENERALI
 - 4.1. IL SISTEMA ORGANIZZATIVO IN GENERALE
 - 4.2. IL SISTEMA DI DELEGHE E PROCURE
 - 4.3. PRINCIPI GENERALI DI COMPORTAMENTO
5. PRINCIPI DI RIFERIMENTO PER I REATI DI IMPIEGO DI LAVORATORI IRREGOLARI
 - 5.1. PROTOCOLLI DI RIFERIMENTO PER L'ASSUNZIONE DI LAVORATORI STRANIERI
 - 5.1.1. PRESENTAZIONE DELLA DOMANDA DI NULLA OSTA ALL'ASSUNZIONE DI LAVORATORE STRANIERO RESIDENTE ALL'ESTERO
 - 5.1.2. RILASCIO DI NULLA OSTA ALL'ASSUNZIONE
 - 5.1.3. RICHIESTA E RILASCIO DEL VISTO D'INGRESSO
 - 5.1.4. INGRESSO IN ITALIA
 - 5.1.5. OBBLIGHI DI COMUNICAZIONE PER ASSUNZIONE
 - 5.1.6. RICHIESTA DEL RINNOVO DI PERMESSO DI SOGGIORNO PRIMA DELLA SCADENZA
 - 5.1.7. ASSUNZIONE DI UN LAVORATORE STRANIERO GIA' SOGGIORNANTE IN ITALIA
 - 5.1.8. DIVIETO DI ASSUNZIONE DI UN LAVORATORE STRANIERO PRIVO DI PERMESSO DI SOGGIORNO
 - 5.1.9. VALIDITA' DEL PERMESSO DI SOGGIORNO PER LO STRANIERO CHE PERDE IL LAVORO
 - 5.2. PROTOCOLLI DI RIFERIMENTO PER L'AFFIDAMENTO, LA GESTIONE E LA VIGILANZA DEI CONTRATTI D'APPALTO, D'OPERA E SOMMINISTRAZIONE
6. I CONTROLLI DELL'O.d.V.
7. TESTO DELL'ART. 25-DUODECIES DEL D.LGS. 231/2001

1. DESTINATARI DELLA PARTE SPECIALE F

La presente Parte Speciale riguarda i comportamenti posti in essere da amministratori, dirigenti e dipendenti di SILAQ SERVICE S.r.l. nonché dai suoi consulenti e partner, coinvolti nei processi sensibili. L'obiettivo della Parte Speciale F è che tutti i destinatari, come sopra individuati, adottino comportamenti conformi a prevenire la commissione dei reati relativi all'impiego di lavoratori irregolari previsti dall'art. 25-duodecies del D. Lgs. 231/01.

2. I DELITTI INERENTI ALL'IMPIEGO DI LAVORATORI IRREGOLARI

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato di impiego di lavoratori irregolari previste dal D. Lgs. 231/01, riportiamo qui di seguito una descrizione, in forma sintetica, dei reati alla cui commissione da parte di soggetti riconducibili alla Società è collegato il regime di responsabilità a carico della stessa.

I reati di seguito descritti sono stati introdotti con l'inserimento, ad opera dell'art. 2 del D. Lgs. 16 luglio 2012 n. 109, dell'art. 25-duodecies del D. Lgs. 231/01 che, rubricato come "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare", così recita: "1. *In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro*".

Il riferimento normativo all'art. 22, comma 12-bis, del D. Lgs. 286/98 (c.d. "Testo Unico dell'Immigrazione") inerisce all'ipotesi specialmente aggravata del delitto di cui al comma 12 del richiamato Testo Unico. E', infatti, disposto che: "12.bis. *Le pene per il fatto previsto dal comma 12 sono Cdamentate da un terzo alla meta:*

- a) *se i lavoratori occupati sono in numero superiore a tre;*
- b) *se i lavoratori occupati sono minori in età non lavorativa;*
- c) *se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale*".

Il richiamato art. 22, comma 12, del D. Lgs. 286/98 stabilisce che:

"12. Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000 euro per ogni lavoratore impiegato."

Le condizioni di particolare sfruttamento di cui al terzo comma dell'art. 603-bis del codice penale sono, oltre a quelle sopra riportate alle lettere a) e b), "l'aver commesso il fatto esponendo i lavoratori intermediati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro".

In sintesi, l'ente che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è perseguibile ai sensi del D. Lgs. 231/01, se i lavoratori occupati sono (circostanze alternative tra di loro):

- a) in numero superiore a tre;
- b) minori in età non lavorativa;
- c) esposti a situazioni di grave pericolo con riferimento alle prestazioni da svolgere e alle condizioni di lavoro.

2.1. CONSIDERAZIONI SUL REATO DI CAPORALATO

Ad una prima lettura, ed in attesa di interpretazioni giurisprudenziali, sembra non rilevare ai fini della responsabilità amministrativa dell'ente il caso dell'utilizzo di lavoratori reclutati tramite intermediari non Cdatorizzati, c.d. "caporali", già soggiornanti in Italia ed in possesso di regolare permesso di soggiorno.

Ad eccezione del comma 3 (1) che specifica le circostanze aggravanti per la configurabilità della responsabilità amministrativa dell'ente, il c.d. "Reato di caporalato" previsto dall'art. 603-bis c.p. "*Intermediazione illecita e sfruttamento del lavoro*" non è direttamente ed interamente richiamato dal D. Lgs. 231/01.

In assenza di tali circostanze aggravanti, il reato in questione - anche non direttamente realizzato, ma sfruttandone il compimento da parte di un intermediario - non dovrebbe essere rilevante ai sensi del D.Lgs. 231/01, a meno che non si arrivi alla realizzazione del più grave reato di "*Riduzione in schiavitù*" di cui all'art. 600 c.p. e dell'art. 25-quinquies del D. Lgs. 231/01 o dell'ulteriore reato di "*Associazione per delinquere*" di cui all'art. 416 c.p. e dell'art. 24-ter del D. Lgs. 231/01.

Resta ferma, in ogni caso, la responsabilità penale delle persone ovvero dell'intermediario e, presumibilmente, anche del datore di lavoro.

2.2. CONSIDERAZIONI SULLA RESPONSABILITÀ SOLIDALE NEGLI APPALTI

Sebbene la responsabilità amministrativa dell'ente per il reato di impiego di lavoratori irregolari da parte di subappaltatori non sia configurabile ai sensi del D. Lgs. 231/01 anche a carico dell'appaltatore, vigendo l'istituto della responsabilità solidale degli appalti per cui l'appaltatore risponde in solido con il subappaltatore sia per i trattamenti retributivi che per i contributi previdenziali e assicurativi (escluso l'obbligo per le sanzioni civili delle quali risponde solo il responsabile dell'inadempimento), gli aspetti legati all'affidamento, alla gestione ed alla vigilanza sui contratti d'appalto, d'opera e somministrazione sono stati ritenuti significativi e, quindi, considerati nella presente Parte Speciale in quanto essi presentano, oggettivamente, un chiaro rilievo in termini di efficace contrasto all'impiego di lavoratori stranieri irregolari.

3. PROCESSI SENSIBILI

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-duodecies del D.Lgs. 231/01.

I settori / processi / attività esposti maggiormente a rischio per i reati di impiego di lavoratori irregolari possono essere suddivisi in macrocategorie:

- selezione e assunzione di lavoratori stranieri;
- affidamento, gestione e vigilanza sui contratti d'appalto, d'opera e somministrazione;
- Processi ed Attività Sensibili;
- Selezione e assunzione del personale;
- Stipula e gestione di contratti e ordini di acquisto;
- Vigilanza sui lavori affidati e sulla somministrazione di manodopera.

Settori Aziendali maggiormente interessati:

- Cda;
- Procuratore Institorio;
- Responsabile del Servizio di Prevenzione e Protezione;
- Risorse Umane e Organizzazione;

- Acquisti;

4. PRINCIPI DI RIFERIMENTO GENERALI

4.1. IL SISTEMA ORGANIZZATIVO IN GENERALE

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

- formale attribuzione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità; chiara descrizione delle linee di riporto;
- conoscibilità, trasparenza e pubblicità dei poteri e ruoli attribuiti;

Le procedure devono essere caratterizzate dai seguenti elementi:

- separazione all'interno di ciascun processo tra il soggetto che assume la decisione, il soggetto che esegue tale decisione ed il soggetto al quale è affidato il controllo del processo (c.d. segregazione delle funzioni);
- traccia scritta di ciascun passaggio rilevante del processo (c.d. tracciabilità);
- adeguato livello di formalizzazione.

4.2. IL SISTEMA DI DELEGHE E PROCURE

Il sistema di deleghe e procure societarie deve rispettare i seguenti requisiti essenziali:

tutti coloro che, in nome e per conto della Società, intrattengono rapporti verso l'esterno devono essere dotati di una procura e/o di una delega formale sempre rigorosamente aggiornata e rispettosa dei seguenti requisiti. Ciascuna procura o delega deve definire in modo specifico ed inequivoco:

- i poteri del delegato, precisandone in concreto l'ampiezza ed i limiti;
- il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;

L'ampiezza di ciascuna procura e/o delega va correlata alle responsabilità e ad un'adeguata posizione del procuratore / delegato nella struttura organizzativa aziendale;

Qualsiasi comportamento tenuto dal procuratore / delegato in violazione dei limiti assegnatigli o di altre disposizioni di legge o aziendali, con particolare riferimento ai comportamenti che possano fondatamente coinvolgere la Società nei reati di cui alla presente Parte Speciale, e cCdas di revoca immediata dei poteri conferiti.

4.3. PRINCIPI GENERALI DI COMPORTAMENTO

Gli amministratori ed i dipendenti di SILAQ SERVICE S.r.l., i consulenti e partner, sono tenuti, nella misura necessaria allo svolgimento delle attività di competenza, a osservare i seguenti principi generali:

stretta osservanza delle leggi e dei regolamenti che disciplinano le attività aziendali con particolare riferimento alle attività a rischio per i reati di impiego di lavoratori irregolari;

- stretta osservanza delle regole definite dal Codice Etico, dal presente Modello, dalle procedure e norme di comportamento interne ed, in particolare, delle norme e delle prassi operative definite dalla Procedura Interna denominata "Qualità-Ambiente-Sicurezza";
- svolgimento delle attività sulla base di criteri di massima correttezza e trasparenza;
- redazione e conservazione della documentazione necessaria a fornire evidenza del rispetto delle prescrizioni in materia di selezione e assunzione dei lavoratori stranieri ed a consentire un controllo efficace sui comportamenti e sulle attività della Società e dei suoi subappaltatori;
- immediata segnalazione all'O.d.V. di qualsiasi circostanza o comportamento posto

- in essere da soggetti correlati a SILAQ SERVICE S.r.l. che destino il sospetto di irregolarità nell'impiego di lavoratori stranieri.

Conseguentemente, è vietato:

- porre in essere, collaborare o dare cCdasà alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle richiamate dall'art. 25-duodecies del D. Lgs. 231/01;
- violare le regole contenute nelle procedure e, in generale, nella documentazione adottata in attuazione dei principi di riferimento previsti nella presente Parte Speciale;
- violare i principi previsti nel Codice Etico;
- violare le norme e le prassi operative definite dalla Procedura Interna denominata "Qualità-Ambiente-Sicurezza";
- porre in essere qualsiasi situazione il cui scopo si rivolga o si risolva essenzialmente nell'impiego di lavoratori irregolari.

5. PRINCIPI DI RIFERIMENTO PER I REATI DI IMPIEGO DI LAVORATORI IRREGOLARI

L'attuazione delle regole e dei divieti elencati nel precedente capitolo richiede – con riferimento alle singole attività sensibili individuate all'interno di SILAQ SERVICE S.r.l. - l'adozione di specifici protocolli aziendali che definiscano gli standard a cui la Direzione e le aree organizzative della Società devono, per quanto di loro competenza, conformarsi nello svolgimento delle attività aziendali.

Facendo salvo il rigoroso rispetto del Codice Etico, delle norme e delle prassi aziendali, di seguito sono descritti i protocolli adottati da SILAQ SERVICE S.r.l. al fine di prevenire le fattispecie di reato di cui alla presente Parte Speciale F.

5.1. PROTOCOLLI DI RIFERIMENTO PER L'ASSUNZIONE DI LAVORATORI STRANIERI

5.1.1. PRESENTAZIONE DELLA DOMANDA DI NULLA OSTA ALL'ASSUNZIONE DI LAVORATORE STRANIERO RESIDENTE ALL'ESTERO

Per instCdarare un rapporto di lavoro subordinato a tempo indeterminato, determinato o stagionale con un cittadino extracomunitario residente all'estero, il datore di lavoro, italiano o straniero regolarmente soggiornante, deve presentare una specifica richiesta nominativa di nulla osta, cioè di Cdatorizzazione, all'assunzione presso ogni Prefettura – Ufficio territoriale del governo (Sportello unico competente) per il luogo in cui l'attività lavorativa dovrà effettuarsi, compilata su un apposito modulo: solo a partire dalla data stabilita dal "decreto flussi" che fissa le quote di ingresso per motivi di lavoro subordinato, cioè il numero di lavoratori stranieri Cdatorizzati ad entrare in Italia;

solo per via telematica, tramite un personal computer dotato di connessione ad Internet e di un indirizzo di posta elettronica valido e funzionante.

Per la compilazione e l'invio della domanda si deve seguire correttamente la specifica procedura illustrata sul sito web del Ministero dell'Interno (www.interno.it).

Le operazioni di compilazione - che deve essere predisposta nel periodo precedente il giorno dell'invio – e di invio delle domande possono essere materialmente effettuate anche da una persona diversa dal datore di lavoro e non necessariamente tramite un pc aziendale; per l'effettuazione di tutte le operazioni il datore di

lavoro, comunque, può rivolgersi anche ad associazioni di categoria o a patronati accreditati per questo compito.

Le domande si possono inviare solo dal pc su cui è stato compilato il modulo.

Poichè le quote di ingresso per motivi di lavoro subordinato sono ampiamente inferiori alle domande e viene stabilita una graduatoria in base all'ordine di presentazione, per vedere accolta la domanda è assolutamente necessario effettuare l'invio della domanda nei primi minuti successivi all'avvio della "lotteria delle quote", nel giorno stabilito dal decreto flussi.

Nella domanda il datore di lavoro si impegna a garantire al lavoratore straniero il trattamento retributivo ed assicurativo previsto dalle leggi vigenti e dai contratti collettivi nazionali di lavoro applicabili, ad assicurare al lavoratore un'adeguata sistemazione ovvero un alloggio che rientri nei parametri previsti dalle norme provinciali per gli alloggi di edilizia residenziale pubblica e ad effettuare entro i termini di legge le comunicazioni obbligatorie relative al rapporto di lavoro.

5.1.2. RILASCIO DI NULLA OSTA ALL'ASSUNZIONE

Il nulla osta all'assunzione viene rilasciato dallo Sportello Unico Immigrazione (SUI). Lo Sportello Unico:

- acquisisce il parere del Questore circa la sussistenza, nei confronti del lavoratore straniero, dei motivi ostativi al rilascio del nulla osta;
- acquisisce il parere della Direzione Provinciale del Lavoro circa la sussistenza o meno dei requisiti minimi contrattuali e della capienza reddituale del datore di lavoro.

In caso di parere negativo da parte di almeno uno degli Uffici, lo Sportello rigetta l'istanza.

In caso di parere favorevole:

- convoca il datore di lavoro per la consegna del nulla osta (il datore di lavoro deve presentare 2 marche da bollo, il documento d'identità ed una fotocopia di questo e la fotocopia del frontespizio del passaporto del lavoratore che si intende assumere) e per la firma del contratto (che successivamente viene sottoscritto anche dal lavoratore straniero dopo l'ingresso in Italia);
- trasmette per via telematica la documentazione agli uffici consolari.

È importante sapere che il nulla osta al lavoro subordinato ha validità pari a 6 mesi dalla data del rilascio, durante i quali il lavoratore deve fare ingresso in Italia, presentarsi allo Sportello e stipulare il contratto.

5.1.3. RICHIESTA E RILASCIO DEL VISTO D'INGRESSO

Il datore di lavoro invia il nulla osta al lavoratore straniero, che richiede all'ambasciata o al consolato italiani il rilascio del visto di ingresso per motivi di lavoro subordinato, presentando il passaporto, il nulla osta ed altri documenti eventualmente richiesti.

Il visto deve essere richiesto entro i 6 mesi di validità del nulla osta. Se vi sono i requisiti previsti, entro 30 giorni dalla presentazione della domanda al cittadino straniero viene rilasciato il visto di ingresso per motivi di lavoro subordinato non stagionale che consente di entrare regolarmente in Italia.

Il lavoratore straniero che si intende assumere deve trovarsi nel Paese di provenienza. Se il lavoratore straniero soggiorna irregolarmente in Italia, l'assunzione è possibile solo seguendo la normale procedura: il lavoratore deve comunque rientrare nel suo Paese per ottenere il rilascio del necessario visto d'ingresso.

5.1.4. INGRESSO IN ITALIA

Dopo che il lavoratore straniero è entrato regolarmente in Italia, presso il Centro per l'impiego territorialmente competente, sottoscrive il contratto di soggiorno, già sottoscritto dal datore di lavoro in occasione della consegna del nulla osta.

Quindi, il lavoratore straniero entro 8 giorni lavorativi dall'ingresso deve richiedere il rilascio del permesso di soggiorno per lavoro subordinato: la domanda, compilata su apposito modulo e con allegati i documenti richiesti, deve essere presentata ad uno degli uffici postali abilitati, che rilascia la ricevuta.

Se non viene richiesto entro 8 giorni lavorativi, il permesso di soggiorno viene rifiutato ed il cittadino straniero viene espulso, a meno che il ritardo non sia provocato da documentate cCdase di forza maggiore (ad esempio, malattia o incidente).

Per l'avvio del rapporto di lavoro, in attesa del rilascio del primo permesso di soggiorno, basta la ricevuta rilasciata dalla posta.

5.1.5. OBBLIGHI DI COMUNICAZIONE PER ASSUNZIONE

Sottoscritto il contratto di soggiorno ed accertato il possesso da parte del lavoratore della ricevuta postale della domanda di rilascio del permesso di soggiorno, e possibile avviare il rapporto di lavoro, dopo avere rispettato alcuni obblighi di comunicazione.

Il datore di lavoro deve:

- comunicare l'instCdarazione del rapporto di lavoro al Centro per l'impiego, competente per la sede di lavoro, il giorno precedente all'inizio dell'attività, inviando per via telematica lo specifico modello "Unificato-Lav". Questa comunicazione vale anche per l'INAIL e per l'INPS;
- se concede al lavoratore l'uso di un'abitazione a qualunque titolo (ospitalità, affitto, comodato), presentare la specifica comunicazione di "cessione di fabbricato" entro 48 ore all'Cdatorità di pubblica sicurezza: alla Questura o al Commissariato di polizia (mod. Cessione di fabbricato), o al Sindaco nei comuni in cui non è presente un presidio della Polizia di Stato (Mod. Comunicazione al Sindaco di ospitalità o di cessione di immobili).

5.1.6. RICHIESTA DEL RINNOVO DI PERMESSO DI SOGGIORNO PRIMA DELLA SCADENZA

Il permesso per motivi di lavoro subordinato ha una durata pari a quella prevista dal contratto di soggiorno e, comunque, non superiore a 2 anni, se il contratto è a tempo indeterminato, e ad 1 anno, nel caso di un lavoro a tempo determinato.

Prima della scadenza del permesso di soggiorno, pertanto, il lavoratore straniero deve presentare ad uno degli uffici postali abilitati la domanda di rinnovo, compilata su apposito modulo ed allegando i documenti richiesti.

E' necessario presentare la domanda di rinnovo prima della scadenza del permesso e, comunque, assolutamente prima che passino 60 giorni dalla scadenza del vecchio permesso. Se trascorrono più di 60 giorni, il rinnovo del permesso di soggiorno può essere rifiutato ed il cittadino straniero può essere espulso. L'ufficio postale rilascia la ricevuta che, in attesa del rilascio del nuovo permesso di soggiorno, garantisce al lavoratore straniero sostanzialmente gli stessi diritti di un permesso ancora valido: in particolare rimane regolarmente in vita il rapporto di lavoro. Quindi, purchè il lavoratore abbia presentato la domanda di rinnovo entro i termini stabiliti e sia in possesso della ricevuta postale, la scadenza del permesso di soggiorno non provoca la cessazione o la sospensione del rapporto di lavoro.

5.1.7. ASSUNZIONE DI UN LAVORATORE STRANIERO GIÀ SOGGIORNANTE IN ITALIA

Il datore di lavoro può assumere anche lavoratori stranieri già soggiornanti in Italia, purchè siano in possesso di un valido documento di soggiorno che abilita a prestare lavoro.

Può essere legalmente assunto, pertanto, il cittadino straniero munito di:

- permesso di soggiorno europeo per soggiornanti di lungo periodo (e il titolare di soggiorno di durata illimitata che ha sostituito la vecchia “carta di soggiorno”);
- permesso di soggiorno che abilita al lavoro e, quindi, permesso per lavoro subordinato o Cdatonomo, per attesa occupazione, per famiglia, per “assistenza minore”, per asilo politico, per protezione sociale, per motivi umanitari;
- ricevuta postale rilasciata dietro presentazione della domanda di rinnovo di un permesso di soggiorno che abilita al lavoro (quindi di uno dei permessi sopra indicati);
- ricevuta postale rilasciata dietro presentazione della domanda di rilascio del primo permesso di soggiorno, ma solo per motivi di lavoro subordinato o di attesa occupazione e non, pertanto, per altri motivi.

Può essere assunto anche il cittadino straniero titolare di un permesso di soggiorno per motivi di studio, ma solo per rapporti di lavoro subordinato per un tempo non superiore a 20 ore settimanali, cumulabili per 52 settimane in modo da non superare, comunque, il limite di 1.040 ore in un anno.

La procedura di assunzione di un lavoratore straniero già regolarmente soggiornante, nei casi legalmente previsti, prevede la preventiva stipulazione del contratto di soggiorno sullo specifico modello per l'assunzione di stranieri già soggiornanti in Italia. Le parti del rapporto devono solo conservare una copia di contratto, che non deve essere inviato o consegnato a nessun ente.

Altri obblighi (già esaminati) per l'assunzione di un lavoratore al primo ingresso in Italia:

- obbligo di comunicare l'assunzione al Centro per l'impiego, competente per la sede di lavoro, il giorno precedente all'inizio dell'attività, inviando per via telematica lo specifico modello “Unificato-Lav”;
- obbligo di comunicare all'Cdatorità di pubblica sicurezza (presidio della Polizia di Stato o Sindaco) l'ospitalità o la cessione di un'abitazione a qualunque titolo.

5.1.8. DIVIETO DI ASSUNZIONE DI UN LAVORATORE STRANIERO PRIVO DI PERMESSO DI SOGGIORNO

Il datore di lavoro non può impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale.

Non è legale nemmeno l'impiego di uno straniero in Italia per motivi di turismo, anche se regolarmente munito della prescritta dichiarazione di presenza.

5.1.9. VALIDITA DEL PERMESSO DI SOGGIORNO PER LO STRANIERO CHE PERDE IL LAVORO

Se un lavoratore straniero subordinato perde il posto di lavoro, anche per dimissioni, il suo permesso di soggiorno rimane valido per almeno un anno. In sostanza il lavoratore, dopo la perdita dell'occupazione, può essere iscritto nelle liste di collocamento per tutta la residua validità del permesso e comunque, salvo che si tratti di permesso stagionale, per un periodo non inferiore a un anno.

5.2. PROTOCOLLI DI RIFERIMENTO PER L’AFFIDAMENTO, LA GESTIONE E LA VIGILANZA DEI CONTRATTI D’APPALTO, D’OPERA E SOMMINISTRAZIONE

Oltre ai principi generali di comportamento definiti al precedente punto 4.3., dovranno essere attuate specifiche procedure per:

- la verifica preliminare dell' idoneità tecnico professionale delle imprese esecutrici e dei lavoratori Cdatonomi accedenti al cantiere ai sensi di quanto previsto dall'art. 26 comma 1 lettera a) del D. Lgs. 81/08 e s.m.i. (c.d. Testo Unico Sicurezza);
- l'acquisizione dell'elenco aggiornato degli addetti presenti in cantiere per l'esecuzione dei lavori affidati all'impresa esecutrice e relativa verifica documentale di regolarità;
- la vigilanza sull'effettivo personale dell'impresa esecutrice presente in cantiere con verifica delle generalità ovvero dei dati indicati nei tesserini di riconoscimento a fronte di quelli dichiarati e ufficialmente comunicati attraverso l'elenco di cui sopra.

6. I CONTROLLI DELL'O.d.V.

Fermo restando il potere discrezionale dell'O.d.V. di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'O.d.V. effettua periodicamente controlli a campione sulle attività connesse ai processi sensibili ai reati di impiego di lavoratori irregolari diretti a verificare la loro corretta esecuzione in relazione ai principi espressi nel presente documento ed, in particolare, alle procedure interne in essere. Per l'effettuazione di tali controlli periodici, l'O.d.V. si avvale, altresì, della collaborazione delle altre funzioni aziendali.

Si ribadisce che all'O.d.V. viene garantita la libertà di accesso a tutte attività aziendali e la disponibilità di consultazione e/o acquisizione di tutta la documentazione rilevante.

7. TESTO DELL'ART. 25-DUODECIES DEL D.LGS. 231/2001

Art. 25-Duodecies "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare:(1)

1. In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro.

(1) Art. 2, Decreto legislativo n. 109 del 16 luglio 2012 (in vigore dal 9 agosto 2012), rubricato: "Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare".

PARTE SPECIALE “G”

REATI TRIBUTARI (art. 25-quinquedecies del D.Lgs. 231/01)

INDICE

- Introduzione e funzione della parte speciale di reati tributari
- Criteri per la definizione di reati tributari
- Le fattispecie di reato richiamate dal D.Lgs. 231/2001
- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Dichiarazione fraudolenta mediante altri artifici (Art. 3 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Dichiarazione infedele (Art. 4 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Omessa dichiarazione (Art.5 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Emissione di fatture o altri documenti per operazioni inesistenti (Art.8 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- Occultamento o distruzione di documenti contabili (Art.10 D.Lgs 74 modificato da art. 39 del D.L. 124 del 26 ottobre 2019)
- sottrazione fraudolenta al pagamento di imposte (Art.11 D.Lgs 74 e s.m.)
- Casi particolari di confisca (Art.12-ter aggiunto dall’ art. 39 del D.L. 124 del 26 ottobre 2019)
- Le attività sensibili relative ai reati tributari
- Organi e funzioni aziendali coinvolte
- Principi e regole di comportamento
- Principi e norme generali di comportamento
- I controlli dell’Organismo di Vigilanza

- Introduzione e funzione della parte speciale di reati tributari

La presente parte speciale si riferisce ai reati tributari di cui all’art. 25-quinquedecies del D.Lgs. n. 231/2001 e ha come obiettivo che tutti i destinatari, ossia amministratori, dirigenti e dipendenti aziendali nonché consulenti e collaboratori, adottino regole di condotta conformi a quanto prescritto dal D. Lgs. n. 231/2001 al fine di prevenire il verificarsi dei reati sopra richiamati

In particolare, la presente Parte Speciale ha lo scopo di:

- Fornire le regole di comportamento e le procedure che gli amministratori, i dirigenti ed i dipendenti, nonché i consulenti, liberi professionisti e partner aziendali sono tenuti ad osservare ai fini della corretta applicazione del Modello
- Fornire all’Organismo di Vigilanza ed ai responsabili delle altre funzioni aziendali che cooperano con il medesimo, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

- Criteri per la definizione di reati tributari

La fattispecie del reato è posta in relazione alla commissione del delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2 del Decreto Legislativo del 10 marzo 2000, n.74 e modificato dall'art. 39 Decreto Legge n. 124 del 26 ottobre 2019 coordinato con la Legge di conversione n.157 del 19 dicembre 2019.

Le fasi di preparazione del reato sono:

- L'approntamento della falsa documentazione con la registrazione delle spese nelle scritture contabili e l'utilizzo di esse per giungere al calcolo dell'imponibile per imposte
- La indicazione in una delle dichiarazioni previste dalla legge degli elementi riportati nella documentazione fittizia,

mentre la fase di commissione si realizza nel momento in cui viene presentata la dichiarazione compilata utilizzando la falsa documentazione consistente in fatture o altri documenti come scontrini, ricevute fiscali, etc. riguardanti operazioni inesistenti.

- Le fattispecie di reato richiamate dal D. Lgs. 231/2001

La presente Parte Speciale si riferisce a comportamenti posti in essere dai dipendenti e dagli organi sociali aziendali, nonché dai suoi collaboratori esterni e dai suoi Partner

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 aziendali che cooperano con tale organismo, gli strumenti esecutivi necessari affinché gli stessi possano esercitare le attività di controllo, monitoraggio e verifica

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

La presente Parte Speciale si riferisce alla "dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti" aggiunta nel corpus del Decreto Legislativo 231/01 con l'Art. 25-quinquedecies dall'art. 39 del Decreto Legge n. 124 del 26 ottobre 2019 specificando le sanzioni nei confronti di persone giuridiche, società e associazioni per delitti appunto inerenti al reato di cui sopra.

Nei casi previsti dai commi 1 e 2 dei sotto indicati articoli, si applicano inoltre le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e) del D. Lgs 231/01:

- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) il divieto di pubblicizzare beni o servizi.

Si descrivono qui di seguito le principali fattispecie di reato con le relative sanzioni pecuniarie a carico degli enti richiamate dal Decreto all'art. 25-quinquedecies.

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2 D.Lgs 74 modificato da art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 2 del D.Lgs 74 modificato al comma 1, con l'aggiunta del comma 2-bis.

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.
2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dal comma 1, la sanzione pecuniaria fino a cinquecento quote.

Per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dal comma 2-bis, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

- Dichiarazione fraudolenta mediante altri artifici (Art. 3 D.Lgs 74 modificato da art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 3 del D.Lgs 74 modificato al comma 1

1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni

relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

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

2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali. Per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

- Dichiarazione infedele (Art. 4 D.Lgs 74 modificato da art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 4 del D.L.gs 74 modificato ai commi 1 e 1-ter

1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore a dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

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

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

- Omessa dichiarazione (Art.5 D.Lgs 74 modificato da art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 5 del D.L.gs 74 modificato ai commi 1 e 1-bis

1.È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

-Emissione di fatture o altri documenti per operazioni inesistenti (Art.8 D.Lgs 74 modificato da art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 8 del D.L.gs 74 modificato al comma 1 e con l'aggiunta del comma 2-bis

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

3....

Per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dal comma 1, la sanzione pecuniaria fino a cinquecento quote.

Per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dal comma 2-bis, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

- occultamento o distruzione di documenti contabili (Art.10 D.Lgs 74 modificato da art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 10 del D.L.gs 74 modificato al comma 1

1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

- sottrazione fraudolenta al pagamento di imposte (Art.11 D.Lgs 74)

Si riporta il testo dell'articolo 11 del D.L.gs 74 e s.m.

1. Salvo che il fatto costituisca più grave reato è punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

2. Salvo che il fatto costituisca più grave reato è punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

Per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

- Casi particolari di confisca (Art.12-ter aggiunto dall' art. 39 del D.L. n.124 del 26 ottobre 2019)

Si riporta il testo dell'articolo 12-ter aggiunto dal D.L. n.124 e inserito dopo l'art. 12- bis del D.Lgs 74

1. Nei casi di condanna o di applicazione della pena a norma dell'articolo 444 del codice di procedura penale per i delitti di seguito indicati, si applica l'articolo 240-bis del codice penale quando:

- a) l'ammontare degli elementi passivi fittizi è superiore a euro duecentomila nel caso del delitto previsto dall'articolo 2
- b) l'imposta evasa è superiore a euro centomila nel caso del delitto previsto dall'articolo 3
- c) l'importo non rispondente al vero indicato nelle fatture o nei documenti è superiore a euro duecentomila nel caso del delitto previsto dall'articolo 8
- d) l'ammontare delle imposte, delle sanzioni e degli interessi è superiore ad euro centomila nel caso del delitto previsto dall'articolo 11, comma 1
- e) l'ammontare degli elementi attivi inferiori a quelli effettivi o degli elementi passivi fittizi è superiore a euro duecentomila nel caso del delitto previsto dall'articolo 11, comma 2.

- Le attività sensibili relative ai reati tributari

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001

L'analisi svolta nel corso del Progetto ha permesso di individuare le attività della Società che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dall'art. 25-quinquedecies del D.Lgs. 231/2001.

Prima dell'introduzione di questo articolo in merito agli illeciti amministrativi venivano analizzate quelle aree aziendali in cui potevano annidarsi i reati di riciclaggio, corruzione tra privati, illecite operazioni sul capitale sociale, etc.; con l'articolo 25-quinquedecies le stesse aree aziendali sono quelle più sensibili e quindi da monitorare in riferimento ai reati tributari per l'ottenimento di vantaggi fiscali illeciti sia in materia di IVA sia in materia di imposte dirette.

Le aree a rischio "diretto" coprono l'intera area amministrativa-contabile di un ente in modo particolare quelle interessate alle operazioni in materia di imposte e di versamenti di IVA.

- Organi e funzioni aziendali coinvolte

In relazione ai reati e alle condotte criminose sopra esplicitate le aree ritenute più specificamente a rischio risultano

essere, anche in riferimento alle attività svolte dall'azienda le seguenti:

- Gestione fatturazione

- Gestione amministrativa
- Gestione di attività collegate ad import ed export
- Gestione fornitori
- Gestione acquisti
- Attività di gestione del personale.

Eventuali integrazioni delle suddette Aree a Rischio potranno essere disposte dall'Amministratore Delegato al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

- Principi e regole di comportamento

Tutti i Processi Sensibili devono essere svolti conformandosi alle leggi vigenti e al codice di condotta aziendale nonché alle procedure aziendali, ai valori e alle regole contenute nel Modello

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

- Principi e norme generali di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali aziendali (e dei Destinatari, Dipendenti, e Consulenti/Partner 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
- Violare i principi e le procedure esistenti in azienda e/o previste nella presente Parte Speciale

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

- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività amministrativo-contabile
- Assicurare che il processo di assunzione ed impiego del personale del settore amministrativo sia motivato da effettive necessità aziendali, che sia condotto in maniera trasparente e documentabile e che sia basato su criteri non arbitrari e quanto possibile oggettivi.
- Assicurare l'esistenza nell'impresa di un sistema sia organizzativo, sia amministrativo-contabile adeguati e che ricomprendano anche un sistema gestionale efficace.

- 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, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale, commessi nell'interesse o a vantaggio dell'azienda, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello

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

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati tributari sono i seguenti:

- Proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati alla presente Parte Speciale
- Monitorare sul rispetto delle procedure per la prevenzione della commissione di reati tributari in costante coordinamento con le funzioni di direzione ed amministrazione del personale
- 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.

PARTE SPECIALE “H”

MODELLI DI CHECKLIST PER L'ATTIVITÀ DELL'ORGANISMO DI VIGILANZA

INDICE

1. Introduzione
2. Il dossier Governance
3. Lettera di attestazione generale all’Organo di Vigilanza
4. Check List 1: Adeguatezza del Modello
5. Check List 2: Valutazione globale del Modello
 - 5.1 Ambiente di controllo
 - 5.2 Valutazione dei rischi.
 - 5.3 Attività di controllo.
 - 5.4 Informazioni e comunicazione.
 - 5.5 Monitoraggio.
6. Reati ed illeciti ex D.lgs. 231/2001
 - 6.1 Reati contro la pubblica amministrazione
 - 6.2 Reati informatici
 - 6.3 Reati societari
 - 6.4 Reati contro la personalità individuale
 - 6.5 Reati in violazione delle norme antinfortunistiche e sulla tutela della igiene e della salute sul lavoro
 - 6.6 Ricettazione e riciclaggio
 - 6.7 Check list Privacy e sicurezza delle informazioni

1. Introduzione

Questo documento (parte integrante del Modello di Gestione e Controllo) definisce il settore di intervento dell'Organo di Vigilanza tra le operazioni effettuate dagli organi di Governance della Società.

Include Liste di Controllo (Checklist) che riguardano sia il comportamento da tenere nei confronti di alcune aree significative dei Reati ed Illeciti inclusi e richiamati nel D. Lgs. 231/2001, sia attinenti a situazioni estranee ai reati specifici ma che possono influenzare il comportamento degli organi di Governance.

Questo documento fa riferimento alle Linee Guida di Confindustria, all'indagine condotta dal Comitato per l'Area D.Lgs 231/2001 dell'Associazione Italiana Internal Cdaditors (AIIA), ai documenti CoSO I e III (Committee of Sponsoring Organizations of the Treadway Commission), ai principi di revisione I.S.A. (International Standards on Cdaditing) nonché alle buone pratiche Gestionali.

Le modalità di verifica del controllo interno aziendale degli organi di Governance possono essere applicati nella fattispecie specifica per assolvere ad una parte dei dettami richiamati dal D. Lgs. 231/2001 e possono coadiuvare l'insieme di procedure o protocolli adottati dell'azienda per creare il Modello con quel carattere "Esimente" richiesto.

2. Il dossier Governance

Questo dossier viene costituito nel primo anno di attività dell'Organismo di Vigilanza e aggiornato negli anni successivi. E' composto dai seguenti documenti:

Relazioni dell'Organo di Vigilanza (Anno Corrente e Anno Precedente)

Lettera di attestazione

Determinazione dell'adeguatezza del Modello già adottato

1. Checklist generale

Checklist dedicate alle singole categorie di reato presupposto

1. Reati contro la Pubblica Amministrazione

2. Delitti informatici e trattamento illecito di dati

3. Reati Societari

4. Reati contro la Personalità Individuale

5. Reati in violazione delle norme antinfortunistiche della tutela della salute sul lavoro

6. Ricettazione e riciclaggio

7. Falsa informativa economico-finanziaria, appropriazioni illecite

Punti da chiarire e note per l'anno successivo (memo ad uso OdV)

3. Lettera di attestazione generale all'Organo di Vigilanza

Modello di lettera di attestazione:

Data

(Organo di Vigilanza destinatario)

1. È nostra la responsabilità che il bilancio sia redatto con chiarezza e rappresenti in modo veritiero e corretto la situazione patrimoniale-finanziaria e il risultato economico d'esercizio, nonché le variazioni intervenute nella situazione patrimoniale-finanziaria.

2. Abbiamo messo a disposizione: dell'OdV

a) tutte le scritture contabili ed i relativi supporti documentali ed informativi;

b) i libri sociali correttamente tenuti ed aggiornati alla data della presente.

3. Non si sono verificate:

- a) irregolarità da parte del Presidente o dei dipendenti della Società che rivestano posizioni di rilievo nell'ambito dei sistemi contabile e di controllo interno;
- b) irregolarità da parte di altri dipendenti della Società, tali da avere un effetto significativo sul bilancio;
- c) notifiche da parte di organismi di controllo pubblico aventi ad oggetto l'inosservanza delle vigenti norme, che possano avere un effetto significativo sul bilancio;
- d) violazioni o possibili violazioni di leggi o regolamenti il cui eventuale effetto avrebbe dovuto essere considerato nel bilancio;
- e) inadempienze di clCdasole contrattuali che possano comportare effetti significativi sul bilancio.

4. Non vi sono:

- a) potenziali richieste di danni o accertamenti di passività che, a parere del nostro legale, possano probabilmente concretizzarsi e quindi tali da dover essere evidenziate nel bilancio come perdite potenziali, così come definite nel successivo punto b);
- b) passività significative, perdite potenziali per le quali debba essere effettuato un accantonamento in bilancio oppure evidenziate nella nota integrativa, e utili potenziali che debbano essere evidenziati nella nota integrativa. Siamo a conoscenza che la dizione «utile o perdita potenziali» si riferisce ad una «potenzialità» ovvero ad una situazione, condizione, circostanza o fattispecie caratterizzate da uno stato d'incertezza, le quali, al verificarsi di uno o più eventi futuri potranno concretizzarsi per la Società in una perdita o un utile, confermando il sorgere di una passività o la perdita totale o parziale di un'attività, ovvero l'acquisizione di una attività o la riduzione di una passività. Tali potenzialità non includono le incertezze legate ai normali processi di stima necessari per valutare talune poste di bilancio in una situazione di normale prosecuzione dell'attività aziendale;
- c) significative operazioni non correttamente rilevate nelle scritture contabili e quindi nel bilancio;
- d) eventi occorsi in data successiva al [DATA CHIUSURA BILANCIO] tali da rendere l'attuale situazione patrimoniale-finanziaria sostanzialmente diversa da quella approvata dagli organi della società tale da richiedere rettifiche o annotazioni integrative al bilancio;
- e) accordi con istituti finanziari che comportino compensazioni fra conti attivi o passivi o accordi che possano provocare l'indisponibilità di conti attivi, di linee di credito, o altri accordi di natura similare;
- f) accordi per il riacquisto di attività precedentemente alienate;
- g) perdite che si debbano sostenere in relazione all'esecuzione o all'incapacità di evadere gli impegni assunti;
- h) perdite che si debbano sostenere in relazione ad impegni assunti per l'acquisto di merci e/o materiali eccedenti il normale fabbisogno o a prezzi superiori a quelli di mercato, o relative alla valutazione di rimanenze di magazzino obsolete;
- i) significativi investimenti fissi non utilizzati.

5. La società non ha programmi futuri o intendimenti che possano alterare significativamente il valore di carico delle attività o delle passività o la loro classificazione o la relativa informativa di bilancio. 6. La società esercita pieni diritti su tutte le attività possedute e non vi sono pegni o vincoli su di esse, né alcuna attività è soggetta a ipoteca o altro vincolo (ad eccezione di quelli evidenziati in bilancio).

7. La Società ha adottato il Modello di Organizzazione e Gestione ex D. Lgs. 231/2001 al fine di garantire a tutti i portatori di interessi il rispetto delle leggi vigenti;

8. La società opera nel rispetto delle normative vigenti, in particolare – ma non limitatamente - in materia di sicurezza e igiene del lavoro nonché di privacy e protezione dei dati;

9. Sono state fornite tutte le informazioni necessarie alla identificazione delle parti correlate e sono state correttamente presentate nel bilancio le operazioni significative con parti correlate con l'indicazione di tutte le informazioni richieste dalle norme di legge e regolamentari in materia;

10. Vi confermiamo che il bilancio d'esercizio e i relativi allegati, che Vi trasmettiamo unitamente alla presente lettera (Vi abbiamo trasmesso in data XXX) sono conformi a quelli che saranno depositati presso la sede sociale. Ci impegniamo inoltre a darVi tempestiva comunicazione delle eventuali modifiche che fossero apportate ai suddetti documenti prima del deposito.

(Inserire di seguito ogni altra attestazione riguardante situazioni specifiche ritenute influenti per la formazione della relazione dell'ODV.)

Distinti saluti

Il Presidente e l.r.

4. Check List 1: Adeguatezza del Modello

Una o più risposte negative implicano la non adeguatezza del modello, che necessita in questo caso di essere rivisto. Le risposte possibili sono sì, no oppure n/a (non applicabile)

Descrizione	Ris.
<ul style="list-style-type: none"> . 1) Il Modello di Organizzazione e Gestione adottato prevede : <ul style="list-style-type: none"> - Delle linee di condotta e comportamento? - Un sistema disciplinare nel caso di violazione del codice etico ? - Un'analisi dei rischi di commissione dei reati ex D.Lgs. 231/2001? - Un riferimento ai protocolli aziendali e di controllo interno che prevengono i rischi identificati? - Un riferimento all'Organismo di Vigilanza (OdV)? . 2) E' previsto l'aggiornamento periodico del modello ? . 3) E' previsto un sistema di informazione iniziale ed una successiva formazione periodica dei destinatari ? . 4) L'OdV e dotato delle seguenti caratteristiche: <ul style="list-style-type: none"> - Cdatonomia? - Indipendenza? - Professionalità? . 5) Nell'OdV è prevista la presenza di almeno un professionista Indipendente? . 6) L'OdV riporta periodicamente al Consiglio di Amministrazione in merito al suo operato? . 7) L'Azienda richiede ai propri Fornitori o Collaboratori l'adesione Scritta al proprio codice di comportamento ? 	

5. Check List 2: Valutazione globale del Modello

La lista di controllo che segue è ispirata ai principi guida indicati e sviluppati nel modello di controllo: Ambiente di controllo, valutazione dei rischi, attività di controllo, informazione e comunicazione, monitoraggio.

5.1 Ambiente di controllo

Costituisce la base per tutti gli altri componenti del sistema di controllo interno. L'integrità, i valori etici, il comportamento del management, l'impegno e le capacità di guida dello stesso determinano il livello di sensibilità del personale fornendo disciplina ed organizzazione nonché integrità e valori etici.

Gli individui, le loro qualità individuali, la loro integrità, i loro valori etici, la loro competenza, e l'ambiente nel quale operano sono l'essenza stessa di qualsiasi organizzazione. Essi sono il motore che aziona l'azienda e le fondamenta su cui essa poggia per questo motivo la direzione e gli organi di governance devono trasmettere il messaggio che l'integrità dell'azienda non può essere oggetto di compromessi. Il "comportamento esemplare del vertice" deve essere il messaggio trasmesso e recepito a tutti i livelli aziendali e quindi lo stile con cui gli organi di governance opera, delega responsabilità e poteri deve essere appropriato.

		Ris.
1	Esiste ed è in uso presso l'azienda un Codice Etico e di Comportamento?	
2.	Gli organi di governance e la direzione comunicano in forma appropriata i principi del Codice Etico e di Comportamento riferiti al fatto che l'integrità dell'azienda non può essere oggetto di compromessi?	
3.	Gli Organi di governance e la direzione tengono e divulgano il concetto di "Comportamento corretto"?	
4.	Esistono direttive e principi di controllo interno ben definiti, per effetto dei quali si riscontra all'interno dell'azienda una consapevolezza diffusa dell'importanza dell'applicazione delle procedure di controllo interno?	
5.	La competenza del personale dell'azienda è commisurata - Ai compiti assegnati? - alle responsabilità richieste?	
6.	Lo stile con cui agiscono gli i organi di governance e la direzione è appropriato? - nella delega dei poteri e responsabilità? - nell'organizzazione della struttura? - Nella gestione del personale? - Nel favorirne la crescita professionale dello stesso?	
7.	Gli Organi di governance e la direzione curano con l'adeguato impegno l'applicazione dei principi sopra descritti ?	—

5.2 Valutazione dei rischi.

Ogni azienda deve essere consapevole dei rischi esterni ed interni che incontra e che deve affrontare nel raggiungimento degli obiettivi. Essa deve porsi obiettivi strategici e specifici per attività commerciali, finanziarie, di produzione, di marketing ed altre; tali attività devono essere reciprocamente integrate in modo che l'organizzazione possa operare in modo coordinato ed armonico. Essa deve anche attivare i meccanismi che consentono di individuare analizzare e gestire i rischi relativi.

5.3 Attività di controllo.

Le varie attività di controllo sono attuate in tutta l'organizzazione ed a tutti i livelli. Le attività di controllo garantiscono agli organi di governance che le direttive e lo spirito etico dell'azienda siano attuati e seguiti nella pratica.

Con l'attività di controllo si favorisce l'applicazione di procedure necessarie per far fronte ai rischi che potrebbero pregiudicare il raggiungimento degli obiettivi aziendali.

Le politiche e le procedure di controllo devono essere applicate a tutte le attività dell'azienda per assicurare che siano attivati efficacemente provvedimenti che il management ritiene necessari per ridurre i rischi connessi alla realizzazione degli obiettivi.

5.4 Informazioni e comunicazione.

Il sistema informativo ed in senso lato le comunicazioni aziendali devono mettere in grado gli organi di governance e tutti i livelli aziendali di assolvere le proprie funzioni. Il personale deve essere messo in grado di assolvere ai propri compiti ed essere adeguatamente edotto sull'importanza del proprio operato all'interno della struttura aziendale. In questo modo le informazioni faranno parte di un sistema integrato per il raggiungimento degli obiettivi aziendali. Intorno alle suddette attività di controllo si collocano i sistemi di comunicazione ed informazione per tutti i settori dell'azienda. Questi consentono al personale la raccolta e lo scambio delle informazioni necessarie alla gestione ed al controllo. I sistemi di informazione e controllo devono essere in grado di individuare e raccogliere le informazioni significative e rilevanti per trasmetterle al personale in modo chiaro per permettere allo stesso di interpretarle ed assolvere ai compiti assegnati

		Ris.
1	<p>Il sistema informativo aziendale è in grado:</p> <ul style="list-style-type: none"> - di individuare e raccogliere le informazioni significative: <p>Finanziarie e contabili Gestione degli incarichi tecnici Anagrafiche degli utenti e dei clienti Tali informazioni sono trasmesse al personale competente ed in una forma che consenta di assolvere i compiti assegnati?</p>	
2.	<p>Il sistema di informazione interna dell'azienda:</p> <ul style="list-style-type: none"> - è efficace e quindi consente a tutti gli utenti di ottenere le informazioni appropriate allo svolgimento del proprio compito? - la comunicazione avviene in modo chiaro in rapporto alle attese ed alle responsabilità dei singoli utenti. - sono predisposte di soddisfare l'esigenza di dar conto dei risultati? 	
3.	<p>Il sistema IT adottato mette in condizione tutti gli utenti interessati di ottenere -</p> <ul style="list-style-type: none"> - informazioni complete? - informazioni attendibili? 	

5.5 Monitoraggio.

Viene instaurato all'interno dell'azienda un sistema di controllo e supervisione continua delle procedure che devono essere valutate ed eventualmente aggiornate. Il controllo può essere continuo (eseguito dagli utenti) o periodico (eseguito dagli organi di vigilanza). La consistenza del monitoraggio sarà determinata dalla valutazione dei rischi e dalla validità dei controlli. Sempre e comunque eventuali carenze, disfunzioni od anomalie dovranno essere segnalate agli organi di governance. L'intero processo deve essere monitorato adeguatamente apportandovi le eventuali modifiche richieste dalle circostanze. In tal modo il sistema può reagire rapidamente in funzione dei cambiamenti che si verificano nel contesto operativo.

		Ris.
1.	Il monitoraggio del sistema di controllo interno è attuato da: Organo di Controllo Organo di Vigilanza Collegio Sindacale Revisore contabile (Società di revisione) Oltre agli organi di vigilanza sopra descritti Sono state introdotte ulteriori procedure di monitoraggio continuo o periodico del funzionamento del sistema di controllo interno?	
2.	Gli scostamenti vengono segnalati, per mezzo di lettera alla direzione, agli organi di governance competenti?	
3.	Le politiche aziendali e le procedure vengono modificate per adeguarle all'evoluzione dell'azienda?	

6. Reati ed illeciti ex D.lgs. 231/2001

Le checklist descritte in questa sezione analizzano in modo specifico blocchi di reati ed illeciti richiamati dal D. Lgs. 231/2001 dall'Art. 24 e 24 bis all'Art. 25 a 25 octies, ritenuti più a rischio di commissione all'interno dell'Ente. Sono elencati i principi generali di condotta che gli organi di Governance devono seguire e nella gestione del rapporto, le procedure da osservare nelle singole operazioni a rischio ed i rapporti con parti terze nonché i comportamenti vietati e sospetti.

6.1 Reati contro la pubblica amministrazione

CORRUZIONE E CONCUSSIONE	
TIPO DI REATO	CONTROLLI CCDATELATIVI
<ul style="list-style-type: none"> • Vendere beni, fornire servizi e realizzare opere per la Pubblica Amministrazione. • Ottenere concessioni, licenze ed autorizzazioni da parte della P.A. • Ottenere trattamenti di favore (ad esempio in sede di conciliazione amministrativa) da parte della Pubblica Amministrazione. • Ottenere trattamenti di favore da parte di autorità di controllo e/o di vigilanza. 	<ul style="list-style-type: none"> • Esplicita previsione tra i principi etici del divieto di pratiche corruttive. • Controllo dei flussi finanziari aziendali. • Controllo della documentazione aziendale e, in particolare, fatture passive (la pratica più diffusa per procurarsi la provvista corrompere è l'utilizzazione di fatture per operazioni inesistenti). • Controlli dei collaboratori esterni e dei consulenti e della congruità dei compensi rispetto a quelli praticati nel mercato di riferimento.
TRUFFA AGGRAVATA AI DANNI DELLO STATO	
TIPO DI REATO	CONTROLLI CCDATELATIVI
<ul style="list-style-type: none"> • Produzione alla P.A. di documenti falsi 	<ul style="list-style-type: none"> • Puntuali attività di controllo gerarchico (incluso sistema

<p>attestanti l'esistenza di condizioni essenziali per partecipare ad una gara, per ottenere licenze, Cdatorizzazioni, ecc.</p>	<p>di deleghe).</p>
<p>FRODE INFORMATICA</p>	
<p>TIPO DI REATO</p>	<p>CONTROLLI CCDATELATIVI</p>
<p>Alterazione di registri informatici della PA per far risultare esistenti condizioni essenziali per la partecipazione a gare ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti o, ancora, per modificare dati fiscali / previdenziali di interesse dell'azienda (es. mod. 770), già trasmessi all'Amministrazione.</p>	<p>Sistema di controlli interni all'azienda che prevedano ai fini del corretto e legittimo accesso ai Sistemi informativi della Pubblica Amministrazione:</p> <ul style="list-style-type: none"> • un adeguato riscontro delle password di abilitazione per l'accesso ai Sistemi Informativi della PA possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche Funzioni/Strutture aziendali; • la puntuale verifica dell'osservanza, da parte dei dipendenti medesimi, di ulteriori misure di sicurezza adottate dalla società; • il rispetto della normativa sulla privacy a tutela del dipendente. Questi meccanismi assumono maggiore pregnanza per quelle società o enti che, sulla base di un rapporto di appalto/concessione con un'Amministrazione pubblica o in qualità di Società miste partecipate da un'Amministrazione/Ente locale e da un privato imprenditore, si assumono l'incarico di realizzare, sviluppare e gestire un Sistema Informativo pubblico o un Sistema Informativo di interesse pubblico.
<p>REATI IN TEMA DI EROGAZIONI PUBBLICHE</p>	
<p>TIPO DI REATO</p>	<p>CONTROLLI CCDATELATIVI</p>
<ul style="list-style-type: none"> • Settore finanziario • Investimenti ambientali • Investimenti produzione • Ricerca ed innovazione tecnologica 	<ul style="list-style-type: none"> • Specifica previsione del codice etico. • Diffusione del Codice Etico verso tutti i dipendenti. • Programma di informazione/formazione periodica del dipendente. Responsabilizzazione esplicita, riportata in ordine di servizio della Funzione competente e nel contesto delle relative procedure aziendali, delle funzioni competenti alla predisposizione dei progetti e delle relative istanze. • Separazione funzionale fra chi gestisce le attività realizzative e chi presenta la documentazione di avanzamento. • Specifiche attività di controllo gerarchico su documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali

	<p>dell'azienda che presenta il progetto).</p> <ul style="list-style-type: none"> • Coerenza delle procure verso l'esterno con il sistema delle deleghe. • Esclusione esplicita, nel sistema delle procure, della "richiesta di denaro o altra utilità a terzi". • Meccanismi di pubblicità verso gli interlocutori esterni delle procure. Puntuali attività di controllo gerarchico, previste altresì in sede di Ordine di servizio delle Funzioni competenti che partecipano al processo di acquisizione di beni e servizi per la Società.
--	---

Descrizione	Ris.
<p>La presente checklist dispone a carico degli Esponenti Aziendali, dei Consulenti, dei Partner e parti terze in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti del Gruppo nell'ambito dell'espletamento delle attività considerate a rischio, di attenersi ai seguenti principi generali di condotta:</p> <ol style="list-style-type: none"> 1) astenersi dal porre in essere comportamenti tali da integrare i Reati sopra descritti (Artt. 24 e 25 del Decreto); 2) porre in essere, promuovere, collaborare, o dare cCda a comportamenti tali da integrare le fattispecie rientranti tra i Reati ed Illeciti presupposto; 3) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte possano potenzialmente diventarlo; 4) utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati. <p>Gestione del rapporto Assumere o mettere in atto comportamenti</p> <ol style="list-style-type: none"> 1) che nell'esercizio delle attività oggetto delle Cdatorizzazioni/licenze, possano essere finalizzati ad evitare, anche in parte, l'osservanza degli adempimenti di legge/amministrativi o, comunque, a poter disporre di indebiti privilegi; 2) che in sede di adempimenti conseguenti agli obblighi di legge/normativi e di attività di gestione in genere, possano essere diretti a rappresentare alla Pubblica Amministrazione dati/informazioni non corretti, con la finalità di perseguire "posizioni privilegiate" nell'interesse della Società o di eludere obblighi di legge/normativi; 3) che in sede di ispezioni/controlli o verifiche da parte di Cdatorità o Rappresentanti delle Istituzioni, possano essere finalizzati a influenzare indebitamente, nell'interesse della Società, il giudizio/parere di tali Organismi; 4) Nell'espletamento delle rispettive attività e funzioni oltre alle regole di cui al presente Modello, gli Esponenti Aziendali sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti: 	

<ul style="list-style-type: none"> • il Codice etico; • ogni altra documentazione relativa al sistema di controllo interno in essere nella Società; • le procedure per l'assunzione e la formazione del personale. <p>Ai Consulenti, Partner, Fornitori e parti terze deve essere resa nota l'adozione del Modello e del Codice etico da parte del Gruppo.</p> <p>Si prevede a carico dei Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti del Gruppo nell'ambito dell'espletamento delle attività considerate a rischio, l'espresso divieto di: a) effettuare elargizioni in denaro a pubblici funzionari italiani o esteri (o a loro familiari, parenti, affini, amici ecc.);</p>	
---	--

<p>b) distribuire omaggi e regali o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della P.A. (o loro parenti, affini, amici, ecc.), al di fuori di quanto previsto dalla prassi aziendale (vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale).</p> <p>c) promettere od offrire a rappresentanti della Pubblica Amministrazione (o loro parenti, affini, amici, ecc.) la prestazione di consulenze e/o altri servizi che possano avvantaggiarli a titolo personale</p> <p>d) effettuare prestazioni in favore dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;</p> <p>e) riconoscere compensi in favore dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.</p> <p>f) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati.</p> <p>Ai fini dell'attuazione dei comportamenti di cui sopra:</p> <ol style="list-style-type: none"> 1. i rapporti nei confronti della P.A. per le Aree a Rischio devono essere gestiti in modo unitario, procedendo alla nomina di uno o più Responsabili Interni per ogni operazione o pluralità di operazioni; 2. gli incarichi conferiti ai Consulenti devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito; 3. i contratti stipulati con i Fornitori nell'ambito delle Aree a Rischio devono essere redatti per iscritto con l'indicazione del compenso pattuito; 4. nessun tipo di pagamento può essere effettuato in contanti o in natura; 5. le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto; 6. coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione 	
---	--

sull'attuazione degli adempimenti stessi e riferire tempestivamente all' OdV eventuali situazioni di irregolarità.	
--	--

In questa check list la risposta «no» impone lo studio approfondito della procedura, l'analisi delle eventuali implicazioni di verifica riferite alle transazioni specifiche

6.2 Reati informatici

Descrizione	Ris.
<p>Richiedere l'impegno dei Partner. Fornitori e parti terze al rispetto degli obblighi di legge in tema di Reati Informatici e di protezione dei dati. In particolare, l'affidabilità di tali Partner o Fornitori e parti terze deve essere valutata, ai fini della prevenzione dei Reati Informatici anche attraverso specifiche indagini ex ante.</p> <p>Il sistema dei controlli, adattato dalla Società prevede, con riferimento alle singole aree a rischio individuate, una serie di protocolli di controllo di seguito descritti e applicabili a tutte le aree a rischio – deve essere formalizzata una politica in materia di sicurezza del sistema informativo che preveda, fra l'altro:</p> <ul style="list-style-type: none"> – le modalità di comunicazione anche a terzi; – le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi. – deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici. – deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità per l'identificazione e la classificazione degli asset aziendali (ivi inclusi dati e informazioni). – deve essere adottato e attuato uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. – deve essere adottato e attuato uno strumento normativo che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica. – deve essere adottato e attuato uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. 	
<ul style="list-style-type: none"> – deve essere adottato e attuato uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. <p>In particolare, tale strumento normativo deve prevedere:</p> <ul style="list-style-type: none"> – deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. <p><i>Con riferimento all'attività di gestione della Sicurezza fisica l'Ente si conforma ai seguenti principi di</i></p>	

<p><i>controllo:</i></p> <p>Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.</p> <p>Deve essere adottato e attuato uno strumento normativo che disponga l'adozione di controlli al fine di prevenire accessi non Cdatorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.</p>	
---	--

6.3 Reati societari

--	--

FALSE COMUNICAZIONI SOCIALI - FALSE COMUNICAZIONI SOCIALI IN DANNO DELLA SOCIETÀ, DEI SOCI E DEI CREDITORI – FALSO IN PROSPETTO

TIPO DI REATO	CONTROLLI CCDA RELATIVI
<p>1) il Presidente ignora l'indicazione del Responsabile Amministrativo ed altera il bilancio al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 cod. civ.).</p> <p>2) Altre situazioni similari applicate ad altre poste di bilancio</p>	<ol style="list-style-type: none"> 1. Inserimento nel Codice etico di specifiche previsioni riguardanti il corretto comportamento di tutti i dipendenti coinvolti nelle attività di formazione del bilancio o di altri documenti similari. 2. Attività di formazione di base verso tutti i responsabili di funzione, affinché conoscano almeno le principali nozioni sul bilancio. 3. Istituzione di una procedura chiara e tempificata rivolta alle stesse funzioni di cui sopra, con cui si stabilisca quali dati e notizie debbono essere forniti alla Amministrazione; nonché quali controlli devono essere svolti su elementi forniti dall'Amministrazione e da "validare". 4. Previsione dell'obbligo – per il Responsabile di Ufficio che fornisce dati ed informazioni relative al bilancio o ad altre comunicazioni sociali - di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse. Nella dichiarazione andrà di volta in volta asseverato ciò che obiettivamente e concretamente il soggetto responsabile può documentalmente dimostrare (anche a seguito di verifica ex post) sulla base dei dati in suo possesso, evitando, nell'interesse stesso dell'efficacia dei protocolli, affermazioni generali e generiche. 5. Tempestiva messa a disposizione di tutti i componenti dell'CDA, prima dell'approvazione dello

	<p>stesso; il tutto con una documentata certificazione dell'avvenuta consegna della bozza in questione.</p> <p>6. Sottoscrizione, da parte del massimo Vertice Esecutivo, della c.d. lettera di attestazione.</p>
	<p>8. Procedura che preveda almeno una riunione tra il Collegio Sindacale e l'OdV prima della seduta del Consiglio di Amministrazione indetta per l'approvazione del bilancio, che abbia per oggetto tale documento, con relativa stesura di verbale.</p> <p>I risultati dell'attività dell'OdV devono essere riportati, in via normale, al massimo Vertice esecutivo.</p>
<p>IMPEDITO CONTROLLO</p>	
<p>TIPO DI REATO</p>	<p>CONTROLLI CCDA RELATIVI</p>
<p>Attività aziendale: condotta non corretta e non trasparente tenuta da Amministratori di una Società in relazione ad una puntuale richiesta da parte del Collegio Sindacale di tale Società sul rispetto, da parte della Società medesima, di una determinata normativa.</p> <p>La condotta degli Amministratori - che si possono avvalere di propri diretti collaboratori – si può tradurre in azioni che non rispettino la richiesta di informazioni da parte del Collegio sindacale in tema di applicazione alla Società di una specifica normativa mediante l'occultamento, anche accompagnato da artifici, della documentazione utile a rappresentare i processi applicativi in sede aziendale di tale legge (ad esempio, esibizione parziale o alterata di detta documentazione).</p>	<ul style="list-style-type: none"> • Specifica previsione del Codice Etico. • Diffusione del Codice Etico nel contesto dell'intera organizzazione aziendale. • Previsione di apposito sistema sanzionatorio interno aziendale
<p>OPERAZIONI IN PREGIUDIZIO AI CREDITORI</p>	
	<ul style="list-style-type: none"> • Specifica previsione del Codice Etico. • Diffusione del Codice Etico nel contesto dell'intera organizzazione aziendale. • Programma di informazione/formazione periodica degli amministratori, del management e dei dipendenti sulla normativa di Corporate Governance e sui reati/illeciti amministrativi in materia societaria. • Introduzione/integrazione dei principi di disciplina (regolamenti/procedure) in tema di rapporti di

	Corporate Governance e di osservanza della normativa societaria.
--	--

DESCRIZIONE	RIS.
<p>La presente check list dispone a carico degli Esponenti Aziendali, dei Consulenti e dei Partner, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti del Gruppo nell'ambito dell'espletamento delle attività considerate a rischio, di attenersi ai seguenti principi generali di condotta:</p> <ol style="list-style-type: none"> 1. astenersi dal porre in essere comportamenti tali da integrare i Reati sopra descritti (Art. 25-ter del Decreto); 2. astenersi dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle descritte nell'Allegato A o possano potenzialmente diventarlo. 3. utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati in oggetto. 4. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria. <p>In ordine a tale punto, è fatto divieto di:</p> <ol style="list-style-type: none"> (a) predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società (b) omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore. <ol style="list-style-type: none"> 6. osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo. 7. assicurare il regolare funzionamento della società. e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare. <p>In ordine a tale punto, è fatto divieto di:</p> <ol style="list-style-type: none"> a) tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi frodolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione; b) porre in essere, in occasione di assemblee, atti simulati o frodolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare. <p>Principi procedurali da osservare nelle singole operazioni a rischio</p>	

<p>Si indicano di seguito i principi procedurali che in relazione ad ogni singola Area a Rischio gli Esponenti Aziendali sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte dell'OdV.</p> <p>Rapporti con parti terze Nei contratti con i Consulenti, i Partner e parti terze deve essere contenuta apposita c/cdasa che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché del Modello.</p>	
<p>- Tutti i consulenti, fornitori e in generale qualunque soggetto terzo che agisca per conto della Società è tenuto ad evitare qualunque situazione di conflitto di interessi con la stessa, obbligandosi in caso di conflitto a segnalarlo immediatamente alla Società. – E' fatto divieto a tutti i consulenti, fornitori e in generale qualunque soggetto terzo che agisca per conto della Società di compiere qualunque caso in cui da tale comportamento derivi o possa, anche solo in astratto, derivare un qualunque vantaggio o interesse per la Società.</p>	

6.4 Reati contro la personalità individuale

Descrizione	Note
<p>La presente check list prevede a carico dei Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Ente nell'ambito dell'espletamento delle attività considerate a rischio, l'espresso divieto di:</p>	
<ol style="list-style-type: none"> 1. porre in essere, promuovere, collaborare, o dare c/cdasa a comportamenti tali da integrare le fattispecie rientranti tra i Reati contro la personalità individuale; 2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato possano potenzialmente diventarlo; 3. utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati. <p>Principi procedurali specifici</p> <p>Principi procedurali da osservare nelle singole operazioni a rischio Si indicano di seguito i principi procedurali che in relazione ad ogni singola Area a Rischio gli Esponenti Aziendali sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte del OdV:</p> <ol style="list-style-type: none"> 1. si deve richiedere l'impegno dei Partner, Fornitori e parti terze al rispetto degli obblighi di legge in tema di tutela del lavoro minorile e delle donne, condizioni igienico-sanitarie e di sicurezza, diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del 	

<p>Paese in cui essi operano;</p> <p>2. la selezione delle controparti destinate a fornire particolari servizi (quali ad esempio le imprese con alta incidenza di manodopera non qualificata), siano essi Partner, Appaltatori o Fornitori, deve essere svolta con particolare attenzione e se ritenuto necessario in base ad apposita procedura interna. In particolare, l'affidabilità di tali imprese deve essere valutata, ai fini della prevenzione dei Reati.</p> <p>3. in caso di assunzione diretta di personale da parte delle Società, deve essere verificato il rispetto delle norme giuslavoristiche e degli accordi sindacali per l'assunzione e il rapporto di lavoro in generale. Deve essere, altresì, verificato il rispetto delle regole di correttezza e di buon comportamento nell'ambiente di lavoro ed in ogni caso deve essere posta particolare attenzione a situazioni lavorative anormali o abnormi;</p> <p>4. chiunque rilevi una gestione anomala del personale utilizzato dal Partner, è tenuto ad informare immediatamente l'OdV di tale anomalia; 5. nei contratti con i Partner, Fornitori, Consulenti e parti terze deve essere contenuta apposita dichiarazione dei medesimi di non essere mai stati indagati negli ultimi 5 anni in procedimenti giudiziari relativi ai Reati di cui alla presente sezione;</p> <p>6. deve essere rispettata da tutti gli Esponenti Aziendali la previsione del Codice etico diretta a vietare comportamenti tali che siano in contrasto con la prevenzione dei Reati contemplati dal presente Allegato;</p> <p>7. L'Ente è tenuto a dotarsi di strumenti informatici costantemente aggiornati che contrastino l'accesso a siti Internet contenenti materiale relativo alla pornografia minorile (strumenti di content filtering);</p> <p>8. La Società periodicamente richiama in modo inequivocabile i propri Esponenti Aziendali a un corretto utilizzo degli strumenti informatici in proprio possesso;</p> <p>9. nel rispetto delle normative vigenti, la Società si riserva il diritto di effettuare periodici controlli idonei ad impedire l'abuso dei sistemi informativi aziendali o la commissione di Reati attraverso il loro utilizzo;</p> <p>10. La Società valuta e disciplina con particolare attenzione e sensibilità l'organizzazione diretta e/o indiretta di viaggi o di periodi di permanenza in località estere con specifico riguardo a località note per il fenomeno del c.d. "turismo sessuale";</p> <p>11. nel caso in cui si ricevano segnalazioni di violazione delle norme del Decreto da parte dei propri Esponenti Aziendali e/o Collaboratori Esterni, è tenuta ad intraprendere le iniziative più idonee per acquisire ogni utile informazione al riguardo;</p> <p>12. in caso persistano dubbi sulla correttezza di comportamenti dei Collaboratori Esterni, l'ODV emetterà una raccomandazione per l'Amministratore Delegato e/o per gli Organi Direttivi delle Società interessate.</p> <p>Rapporti con parti terze</p>	
--	--

<p>Nei contratti con i Consulenti, i Partner i Fornitori e parti terze deve essere contenuta apposita clCdasola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché del Modello.</p>	
--	--

6.5 Reati in violazione delle norme antinfortunistiche e sulla tutela della igiene e della salute sul lavoro

--

Premessa / Nota importante

--

Le domande proposte in questa checklist sintetizzano la ben più ampia e puntuale attenzione che la Società vorrà porre nel definire e regolamentare questo vasto campo di rischio rivolgendosi a persone od Organizzazioni di sicura competenza al fine di adottare ed applicare procedure tali che evitino l'incorrere nei reati ed illeciti relativi a questa sezione.

La presente checklist dispone a carico dei Destinatari (Esponenti Aziendali, dei Consulenti e delle Parti Terze), in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società nell'ambito dell'espletamento delle attività considerate a rischio, di attenersi ai principi generali di condotta ed a precisi obblighi.

In particolare, nell'espletamento delle attività connesse alle Aree a Rischio, è espressamente vietato ai Destinatari di porre in essere, collaborare o creare i presupposti per la realizzazione di comportamenti che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato e di illecito amministrativo rientranti tra quelle considerate nella sezione Reati ed Illeciti.

Si prevede ora che il Modello di Organizzazione, Gestione e Controllo idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche di cui al D.Lgs. 231/2001, deve essere adottato ed efficacemente attuato assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

Descrizione	Ris.
1) Sistema prevenzionistico	
E' stata formalmente identificata la figura del Datore di lavoro?	
È stato formalmente istituito ed organizzato il SPP (servizio prevenzione protezione	

aziendale)?	
E' composto da un numero sufficiente di addetti rispetto alle caratteristiche dell'Azienda?	
Il SPP è:	
- Totalmente esterno?	
- Totalmente interno?	
- Misto?	
Il Datore di Lavoro ha formalmente designato il RSPP?	
Il RSPP è:	
- Interno a tempo pieno?	
- Interno ma non a tempo pieno?	
- Esterno?	
- Il Datore di lavoro stesso?	
Quale è il titolo di studio del RSPP:	
- LCdarea in discipline tecniche?	
- LCdarea in altre discipline?	

- Diploma scuola media superiore?
- Altro?

Il RSPP possiede capacità e requisiti professionali adeguati ex D.Lgs. n. 195/2003?

Il SPP è composto da altri Addetti oltre il Responsabile del SPP?

Gli Addetti possiedono capacità e requisiti professionali adeguati ex D.Lgs. n. 195/2003?

Il RSPP e gli Addetti hanno la disponibilità di mezzi e di tempo adeguati per espletare i compiti assegnati?
È necessaria la nomina del Medico Competente?

Se sì, il Medico Competente è stato formalmente nominato?

Il Medico Competente è:
un dipendente dell'Azienda?
un collaboratore esterno?

Il Medico Competente è in possesso dei titoli richiesti dalla normativa?

Sono presenti altre consulenze esterne?

- Se sì sono:
- Saltuarie?

- Sistematiche?

Sono stati formalmente designati i lavoratori addetti a compiti speciali quali:

- Antincendio?
- Pronto soccorso?
- Evacuazione rapida – emergenza?

Viene effettuata la riunione annuale da parte del SPP?

- La riunione non viene effettuata.
- La riunione ha carattere solo burocratico e formale.
- La riunione viene adeguatamente preparata.
- La riunione è stata operativa rispetto ad obiettivi indicati con precisione.

Alla riunione periodica sono convocati e partecipano:

- Il Datore di Lavoro o un suo rappresentante?
- Il RSPP?
- Il Medico Competente?
- Il RLS?

La riunione periodica viene documentata / formalizzata?

Descrizione	Ris.
2) Organizzazione	
Esiste un'organizzazione definita del sistema di prevenzione in azienda?	
Chi gestisce tale sistema:	
- Il datore di lavoro?	

- Il RSPP?
- Il Medico Competente?
- Uno o più dirigenti?
- Uno o più preposti?
- Addetti alle emergenze?

Quali sono gli interlocutori abituali del Responsabile del SPP:

- Datore di lavoro?
- Medico Competente?
- Dirigente/i?
- Preposto/i?
- RLS?
- Lavoratori?

L'organizzazione del sistema di prevenzione è:

- Formalizzata con un atto aziendale ufficiale?
- Resa nota e ufficializzata in altro?

- Non formalizzata, ma storicamente consolidata e nota?

Esiste una formalizzazione scritta dell'assetto organizzativo della funzione prevenzione (es. "chi fa che cosa"; quali sono i rapporti tra RSPP, Datore di Lavoro, Dirigenti, Preposti, ecc.)?

- Sì
- In parte
- Minimamente
- No

È definito formalmente un preciso sistema di responsabilità mediante delega di funzioni (deleghe e/o incarichi per dirigenti e preposti)?

Se sì, le deleghe e gli incarichi rispettano i limiti e le condizioni di cui all'art. 16 D.Lgs. 81/2008?

È definito formalmente un preciso sistema di responsabilità per l'applicazione delle misure preventive che individua con chiarezza compiti e funzioni di dirigenti e preposti?

- Sì
- In parte
- Minimamente
- No

È previsto formalmente un sistema aziendale di controllo per la verifica del modo con cui sono attuate le misure preventive e protettive?

- Sì
- In parte
- Minimamente
- No

Chi gestisce tale sistema, ovvero verifica che vengano attuate le misure di prevenzione e di protezione: - Il Datore di lavoro?

- Il RSPP?
- Il Medico Competente?
- Uno o più dirigenti?
- Uno o più preposti?
- Altro:

È stato attivato un sistema informativo aziendale dedicato per la funzione prevenzione esclusi gli strumenti previsti obbligatoriamente per legge (es: registro infortuni, documento di valutazione dei rischi, ecc.)?	
- Sì	
- In parte	
- Minimamente	

- No	
Descrizione	Ris.
3) Conformità legislativa	
Il Datore di Lavoro garantisce la conformità legislativa (acquisizione di documentazioni e certificazioni obbligatorie di legge) per:	
Rapporti di lavoro?	
- Sì	
- In parte	
- No	
Luoghi di lavoro?	
- Sì	
- In parte	
- No	
Impianti?	
- Sì	
- In parte	
- No	
Attrezzature?	
- Sì	
- In parte	
- No	
Descrizione	Ris.
4) Valutazione dei rischi	
Il Datore di Lavoro ha effettuato la valutazione dei rischi?	
Oltre al Datore di lavoro, nel processo valutativo, sono stati coinvolti altri soggetti aziendali quali:	
- RSPP?	
- Medico Competente?	
- Dirigenti?	
- Preposti?	
- Lavoratori?	
La valutazione ha riguardato tutta l'Azienda (o unità produttiva) e tutti i rischi presenti e comprende:	
- I rischi correlati ai luoghi di lavoro?	

- I rischi correlati agli impianti tecnologici?	
- I rischi correlati alle macchine ed attrezzature di lavoro?	

- Il rischio da movimentazione manuale dei carichi?
- Il rischio da videoterminali?
- Il rischio da esposizione ad agenti fisici (rumore)?
- Il rischio da esposizione ad agenti fisici (vibrazioni)?
- Il rischio da esposizione ad agenti fisici (campi elettromagnetici)?
- Il rischio da esposizione ad agenti fisici (radiazioni ottiche artificiali)?
- Il rischio da esposizione ad agenti chimici?
- Il rischio da esposizione ad agenti cancerogeni e mutageni?
- Il rischio da esposizione all'amianto?
- Il rischio da esposizione ad agenti biologici?
- Il rischio da stress lavoro-correlato?
- I rischi riguardanti le lavoratrici in stato di gravidanza?
- Il rischio da atmosfere esplosive?

La valutazione è stata estesa a tutti i lavoratori dipendenti o ad essi equiparati ?

Se no, specificare le principali carenze (indicare i rischi non presi in esame e/o i reparti/lavorazioni non considerati):

In funzione della Valutazione dei Rischi si sono determinati gli obiettivi (misure generali di tutela) concreti da raggiungere (Art. 15 – D.Lgs. n. 81/2008)?

- Sì
- In parte
- Minimamente
- No

E' stato stabilito un programma di attuazione delle misure di prevenzione e protezione previste per il raggiungimento e il mantenimento nel tempo degli obiettivi prefissati (art. 28, comma 2 – D.Lgs. n. 81/2008)?

- Sì
- In parte
- Minimamente
- No

Se no o in parte, specificare le principali carenze:

Esiste un atto conclusivo del processo di valutazione?

- Documento di cui all'art. 17, comma 1 – D.Lgs. n. 81/2008.
- Cdatocertificazione perché si rientra nei casi previsti.

Il documento finale del processo di valutazione comprende:

Descrizione della struttura organizzativa aziendale?

- No

- Sì
- In parte

Descrizione del ciclo produttivo e del layout con planimetria?

- No
- Sì
- In parte

Indicazione e specificazione degli strumenti, dei metodi e dei criteri con cui si è proceduto alla valutazione?

- No
- Sì
- In parte

Individuazione e valutazione di tutti i rischi?

- No
- Sì
- In parte

Individuazione dei lavoratori esposti?

- No
- Sì
- In parte

Indicazione delle misure di prevenzione e protezione adottate ed attuate?

- No
- Sì
- In parte

Programma delle misure di prevenzione e protezione da adottare o da attuare?

- No
- Sì
- In parte

Il programma delle misure ritenute opportune per garantire il mantenimento ed miglioramento nel tempo dei livelli di sicurezza?

- No
- Sì
- In parte

Se si verificano significative variazioni organizzative / processo produttivo / macchine / impianti / sostanze chimiche/metodo di lavoro, è prevista una procedura per l'aggiornamento della valutazione dei rischi?

- No
- Sì

Descrizione	Ris.
5) Prevenzione incendi	
E' stata effettuata la valutazione del rischio di incendio ex D.M. 10/03/98?	
- Luogo di lavoro a basso rischio di incendio	
- Luogo di lavoro a medio rischio di incendio	
- Luogo di lavoro ad alto rischio di incendio	
La valutazione è documentata con una stima peritale?	
L'Azienda svolge un'attività per cui è obbligatorio il C.P.I.?	
L'Azienda è in possesso del Certificato di Prevenzione Incendi o Nulla Osta Provvisorio o Visto Edilizio?	

In Azienda sono presenti infrastrutture ed attrezzature antincendio?

Tali infrastrutture ed attrezzature antincendio sono adeguati alla natura dell'attività, alle dimensioni dell'azienda ed al numero delle persone presenti?

Tali infrastrutture ed attrezzature antincendio sono soggette a controlli periodici? In Azienda sono presenti attrezzature e presidi per il primo soccorso?

Tali attrezzature e presidi di primo soccorso sono adeguati alla natura dell'attività, alle dimensioni dell'azienda ed al numero delle persone presenti?

Tali attrezzature e presidi di primo soccorso sono soggette a controlli periodici?

E' in essere il Registro di Sicurezza Antincendio?

E' previsto un Piano di emergenza?

Se sì:

- Sono definite le modalità di dichiarazione dello stato di emergenza?
- Sono definiti i sistemi di intervento a seconda della localizzazione dell'emergenza?
- Sono definite le modalità di cessata emergenza?
- Sono state esposte le istruzioni da seguire in caso di emergenza e numeri di telefono utili dei servizi pubblici?
- Sono definite le vie di fuga e le uscite di sicurezza?
- E' stato informato tutto il personale sul contenuto del piano di emergenza?

E' previsto un Piano di evacuazione?

Se sì:

- Sono esposte al pubblico le planimetrie di sicurezza?
- E' stato informato tutto il personale sulle modalità di evacuazione?

- Sono state effettuate esercitazioni pratiche?
- Esiste un programma di addestramento periodico all'evacuazione?

Descrizione	Ris.
6) Programmazione e predisposizione delle misure di prevenzione e di protezione	
Esiste un programma formalizzato (sia esso contenuto o no nell'eventuale Documento di valutazione dei rischi) di attuazione delle misure di prevenzione e protezione previste per il miglioramento e il mantenimento nel tempo degli obiettivi prefissati (Art. 15, co. 1 – D.Lgs. n. 81/2008)?	
- No	
- Si	
È stato reso ai RLS?	
- No	
- Si	
È definita in modo chiaro la sua articolazione cronologica?	
- No	
- Si	
- In parte	

I tempi indicati per gli interventi di bonifica sono congrui rispetto a:

- Entità del rischio?
- Complessità della bonifica?

Il programma quali tipi di interventi copre:

a. Tecnici (strutture - locali)?

- No
- Si
- In parte

b. Tecnici (impianti)?

- No
- Si
- In parte

c. Tecnici (macchine)?

- No
- Si
- In parte

d. Tecnici (attrezzature portatili)?

- No

- Sì
- In parte

e. Ergonomici?

- No
- Sì
- In parte

f. Disponibilità \ consegna \ uso DPI?

- No
- Sì
- In parte

g. Interventi organizzativi?

- No
- Sì
- In parte

k. Norme igieniche / comportamentali?

- No
- Sì
- In parte

l. Informazione?

- No
- Sì
- In parte

m. Formazione?	
- No	
- Sì	
- In parte	
n. Strutture di controllo \ vigilanza interna?	
- No	
- Sì	
- In parte	
o. Altro (specificare)?	
- No	
- Sì	
- In parte	

Il programma attuativo degli interventi preventivi e protettivi è integrato con il più ampio contesto della programmazione aziendale dell'attività produttiva (Art. 15, co. 1, lett. b – D.Lgs. 81/2008)?	
- No	
- Sì	
- In parte	

Descrizione

Ris.

7) Informazione

Esiste una pianificazione ed un programma delle attività di informazione?

- No
- Sì
- In parte (solo per alcune lavorazioni \ reparti)

Il programma delle attività garantisce che ciascun lavoratore riceva una informazione adeguata (con i contenuti richiamati dalla legislazione vigente) in relazione alla propria mansione?

- No
- Sì
- In parte (solo per alcune lavorazioni \ reparti)

Sono definiti con chiarezza e divulgati il sistema delle responsabilità e dei compiti associati all'attuazione del programma nonché le modalità operative del sistema di gestione della sicurezza aziendale?

- No
- Sì
- In parte

Le attività di informazione sono state divulgate in una forma adatta a renderle note a tutti i lavoratori?

1. Lavoro a tempo pieno
2. Lavoro a part-time
3. Lavoro intermittente
4. Lavoro in distacco
5. Stagisti
6. Lavoro interinale
7. Contratti a progetto

Sono state previste modalità "dedicate" per i nuovi assunti?

- No
- Sì

È stata data a tutti i lavoratori l'informazione generale:

Sui rischi dell'impresa?

- No
- Sì
- In parte

Sulle misure di prevenzione adottate?

- No
- Sì
- In parte

È stata data a tutti l'informazione specifica:

- Sui rischi specifici?
- Sulle loro conseguenze?
- Sulle norme di sicurezza?
- Sulle misure e disposizioni aziendale?
- Sulla pericolosità di sostanze e preparati?
- Sulle procedure da seguire in emergenza?
- No
- Sì
- In parte

Con quali strumenti è stata fatta:

- Depliant?
- Video?
- Assemblee generali?
- Volantini?
- Incontri di piccolo gruppo?
- Lezioni in Cdala?
- Avvisi in bacheca?
- Assemblee di reparto?
- Altri?

È stata data l'informazione a tutti i lavoratori:

- Sul nominativo del Datore di Lavoro?
- Sul nominativo del responsabile SPP?
- Sul nominativo del Medico Competente?
- Sui nominativi dei lavoratori addetti ai compiti specifici (addetti alle emergenze)?

Descrizione	Ris.
8) Formazione	
Esiste una pianificazione ed un programma delle attività di formazione?	
- No	
- Sì	
- In parte (solo per alcune lavorazioni \ reparti)	

<p>Il programma delle attività garantisce che ciascun lavoratore riceva una formazione adeguata (con i contenuti richiamati dalla legislazione vigente) in relazione alla propria mansione?</p>	
---	--

- No
- Sì
- In parte (solo per alcune lavorazioni\reparti)

È stata fatta a tutti i lavoratori la formazione?

- No
- Sì
- In parte

È avvenuta la formazione dei lavoratori nei seguenti casi:

a. Assunzione?

- No
- Sì
- In parte

b. Trasferimento \ cambio mansione?

- No
- Sì
- In parte

c. Cambiamento o nuovi rischi?

- No
- Sì
- In parte

Quali strumenti formativi sono stati utilizzati per la formazione di tutti i lavoratori:

- Corsi strutturati (lezioni frontali)?
- Corsi strutturati (lavori di gruppo)?
- Corsi strutturati (simulazioni/casi)?
- Singoli seminari monotematici?
- Distribuzione di materiale?
- Esercitazioni pratiche?
- F.a.d. (pacchetti di Cdataapprendimento)?
- Altro (specificare)?

Chi fa / ha fatto la formazione ai lavoratori:

- Datore di lavoro?
- Responsabile SPP?
- Addetti SPP?
- Dirigenti?

- Preposti?
- Medico Competente?
- Servizio aziendale di formazione?
- Consulenti esterni?
- Altri (specificare)?

È prevista e viene effettuata una verifica finale di apprendimento?

- No
- Sì
- In parte

La verifica formale di apprendimento è documentata?	
- No	
- Sì	
Il programma di formazione prevede una verifica del livello di conoscenze/competenza e capacità di adottare comportamenti di sicurezza durante il lavoro, acquisite dai lavoratori con i corsi di formazione sulla sicurezza (art. 18, comma 1 e 37 del D.Lgs. 81/08)?	
- No	
- Sì	
- In programma	
Sono stati fatti corsi di formazione per le figure che necessitano di una formazione aggiuntiva?	
- DL	
- Preposti	
- RSPP (aggiornamento)	
- RLS	
- Addetti antincendio	
- Addetti evacuazione - rapida emergenza	
- Addetti pronto soccorso	
In particolare il RSPP frequenta i corsi di aggiornamento?	
In particolare gli addetti alle emergenze frequentano i corsi di aggiornamento?	
Descrizione	Ris.
9) Sorveglianza sanitaria	
Il Medico Competente partecipa alla valutazione dei rischi e alla gestione del sistema di prevenzione?	
Il MC collabora e partecipa con il datore di lavoro:	

- Alla valutazione dei rischi?	
- Alla predisposizione di misure di tutela?	
- All'attività di informazione e formazione nei confronti dei lavoratori?	
- All'organizzazione del servizio di primo soccorso?	
In Azienda si effettua la sorveglianza sanitaria?	
- No, perché non è obbligatoria a termini di legge	
- No, ma sarebbe obbligatoria a termini di legge	
- Sì	
Il Medico Competente definisce dei protocolli sanitari in funzione della mansione del lavoratore e dei relativi rischi specifici?	
Esiste un programma di sorveglianza sanitaria per tutti i lavoratori a rischio?	
- No	
- Sì	
- In parte	
Vengono eseguiti regolarmente gli accertamenti sanitari:	
- Preventivi (pre assuntivi)?	
- Periodici?	
- Su richiesta dei lavoratori?	

Il MC istituisce, aggiorna e custodisce una cartella sanitaria per ogni lavoratore?

La cartella sanitaria è custodita con salvaguardia del segreto professionale?

I lavoratori sono adibiti alla specifica mansione lavorativa solamente in presenza del prescritto giudizio di idoneità?

I giudizi di idoneità / non idoneità risultano in un registro o strumento ad hoc?

Il Medico Competente fornisce ai singoli lavoratori le informazioni dovute sugli accertamenti e sugli esiti degli stessi?

Il MC invia annualmente alle USL i dati aggregati?

Il Medico Competente a richiesta del lavoratore rilascia copia della documentazione sanitaria?

Alla cessazione del rapporto di lavoro il MC invia all'ISPESL, nei casi previsti, la cartella sanitaria del lavoratore?

Al momento della cessazione del rapporto di lavoro viene consegnata al lavoratore copia della sua cartella?

- No

- Sì

- A richiesta

Il MC partecipa alla riunione periodica e comunica ai presenti i risultati anonimi collettivi della sorveglianza sanitaria effettuata e fornisce indicazioni su significato di detti risultati ai fini della attuazione delle misure per la tutela della salute e dell'integrità psico-fisica dei lavoratori?

Il Medico Competente visita gli ambienti di lavoro almeno una volta all'anno?

Descrizione	Ris.
10) Dispositivi di protezione individuale	
Sono stati identificati i casi in cui è necessario l'uso dei DPI?	
Esiste un elenco con i DPI necessari e con le loro caratteristiche?	
I DPI sono conformi al D. Lgs. n. 475/1992 e s.m.i.?	
- No	
- Sì	
- Solo alcuni	
I DPI sono stati scelti poiché non erano possibili altri interventi preventivi?	
- No	
- Sì	
- Solo alcuni	
I DPI sono adeguati e coerenti ai rischi?	

I DPI tengono conto delle esigenze del lavoratore?

- No
- Sì
- Solo alcuni

I DPI sono forniti a tutti i lavoratori che ne hanno necessità?

La consegna dei DPI è documentata?

I DPI sono mantenuti in buone condizioni di efficienza?

- No
- Sì
- Solo alcuni

I DPI sono sostituiti quando necessario?

Ogni lavoratore che ne ha diritto ha i suoi DPI personali?

È stata attivata un'adeguata informazione ai lavoratori sull'uso dei DPI?

È stata attivata un'adeguata formazione ai lavoratori sull'uso dei DPI?

Sono dotati di istruzioni per l'uso, facilmente comprensibili a tutti i lavoratori interessati?

È richiesto esplicitamente ai preposti di vigilare e pretendere l'uso, se necessario, dei DPI?

Descrizione	Ris.
11) Consultazione e partecipazione	

Sono presenti i Rappresentanti dei lavoratori per la sicurezza?	
Se no, perché?	
I RLS sono:	
- Interni e fanno parte delle RSU?	
- Interni e non fanno parte delle RSU?	
- Interni e fanno parte, in parte, delle RSU?	
- Di bacino o comparto (RLS territoriali, ovvero RLS-T)?	
I RLS ricevono le informazioni sulla valutazione dei rischi e sulle misure di prevenzione?	
- No	
- Sì	
- In parte	
I RLS ricevono le informazioni degli organi di vigilanza?	
Alla riunione periodica partecipano anche li RLS?	
Il RLS riceve, su richiesta, informazioni dal MC sul significato della sorveglianza sanitaria?	
Il RLS:	

- Può accedere ai luoghi di lavoro in cui si svolgono le lavorazioni?	
- E' consultato preventivamente e tempestivamente in ordine alla valutazione dei rischi, alla individuazione, programmazione, realizzazione e verifica della prevenzione in azienda?	
- E' consultato sulla designazione del responsabile e degli addetti al servizio di prevenzione, alla attività di prevenzione incendi, al primo soccorso, alla evacuazione dei luoghi di lavoro e del medico competente?	
- E' consultato in merito all'organizzazione della formazione?	
- Riceve, su richiesta, le informazioni e la documentazione aziendale Intrinseco alla valutazione dei rischi e le misure di prevenzione relative, nonché quelle inerenti alle sostanze ed ai preparati pericolosi, alle macchine, agli impianti, alla organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali?	
- Partecipa alla riunione periodica del SPP?	

Descrizione**Ris.****12) Procedure di sicurezza**

Sono previste procedure documentate di lavoro in sicurezza per:

a. Condizioni ordinarie di lavoro?

- No
- Sì
- In parte

b. Manutenzioni occasionali?

- No
- Sì
- In parte

b. Situazioni di emergenza?

- No
- Sì
- In parte

Sono previste specifiche procedure documentate per:

a. Acquisti di attrezzature, sostanze chimiche e DPI?

- No
- Sì
- In parte

b. Gestione impianti, attrezzature, dpi, sostanze pericolose?

- No
- Sì
- In parte

c. Affidare lavori in appalto?

- No
- Sì
- In parte

d. Analisi infortuni e malattie professionali?

- No
- Sì
- In parte

e. Informazione e formazione?

- No
- Sì
- In parte

f. Per gestione maternità e lavoro minorile?

- No
- Sì
- In parte

g. Per le attività di vigilanza interna (Cdadit)?

Le procedure sono state trasmesse ai destinatari:

a. Con trasmissione scritta (ordini, manuale) e/o incontri ad hoc?

- No
- Sì
- In parte

b. Informalmente?

- No
- Sì
- In parte

c. In altro modo (specificare)?

- No
- Sì
- In parte

È previsto un sistema interno di verifica della loro applicazione?

- a. No
- b. Sì, affidato ai dirigenti
- c. Sì, affidato ai preposti
- d. Sì, in altro modo (specificare)?

Esistono specifici piani di sicurezza per:

a. La prevenzione incendi?

- No
- Sì
- In parte

b. L'evacuazione dei lavoratori?

- No

- Sì	
- In parte	
c. Il pronto soccorso?	
- No	
- Sì	
- In parte	
È previsto un sistema di revisione / aggiornamento delle procedura e dei piani?	

Descrizione

Ris.

13) Attrezzature di lavoro

Esistono procedure documentate per la scelta e l'acquisto delle attrezzature di lavoro?

Fra gli elementi presi in esame nella scelta delle attrezzature si fa riferimento a:

- Adeguatezza al lavoro da svolgere?
- Idoneità ai fini della sicurezza e della salute?
- Rischi presenti nell'ambiente di lavoro?
- Rischi derivanti dall'impiego nel luogo di lavoro?
- Esperienza, conoscenza dell'attrezzatura proposta?
- Altro(specificare)?

È definito un programma formalizzato di manutenzione delle attrezzature?

Sono state predisposte le istruzioni d'uso delle attrezzature per le quali la valutazione dei rischi ne ha evidenziato la necessità ai fini della sicurezza?

- No
- Sì
- In parte

Esistono specifiche disposizioni documentate per l'uso "selezionato" di attrezzature che richiedono conoscenze o responsabilità particolari?

Per ciascuna attrezzatura sono fornite ai lavoratori incaricati informazioni / istruzioni d'uso comprensibili, necessarie ai fini della sicurezza?

- No
- Sì
- In parte

Se sì, tengono conto anche delle situazioni anormali prevedibili?

I lavoratori incaricati ricevono una formazione adeguata sull'uso delle attrezzature?

I lavoratori incaricati per l'uso "selezionato" delle attrezzature ricevono un addestramento adeguato e specifico anche in relazione ai rischi verso altre persone?

Descrizione	Ris.
14) Gestione degli appalti	
Esistono lavori in appalto o contratto d'opera effettuati all'interno dell'Ente?	
Se sì, specificare quali:	

- Pulizie
- Manutenzione
- Altro

Viene effettuata la verifica dell'idoneità tecnico-professionale delle ditte appaltatrici?

- No
- Sì, per tutte le ditte
 - Sì, ma solo per alcune ditte

Se sì, tale verifica è documentata in modo adeguato?

Sono state fornite al Datore di Lavoro delle ditte appaltatrici le informazioni sui rischi generali, specifici, sulle misure di prevenzione e di emergenza adottate?

- No
- Sì, per tutte le ditte
- Sì, ma solo per alcune ditte

Se sì, tali informazioni sono state fornite in modo adeguato?

Il Datore di Lavoro:

- coopera all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto degli appalti;
- coordina gli interventi di prevenzione e protezione dai rischi cui sono esposti i lavoratori anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori / attività dell'impresa/e coinvolta/e nell'appalto o più appalti;
- elaborando un unico documento di valutazione dei rischi che indichi le misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi da interferenze?
- No
- Sì, per tutti i casi
- Sì, solo per alcuni casi

Nei contratti di appalto sono specificatamente indicati i costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivante dalle interferenze?

Nel caso si svolgano interventi in contemporanea di più ditte appaltatrici, il datore di lavoro committente (o suoi dirigenti e preposti) garantisce, in modo ufficiale, formale e regolamentato, il coordinamento delle misure preventive?

- No
- Sì, per tutti i casi
- Sì, solo per alcuni casi

Esistono lavori effettuati all'esterno dell'unità produttiva ove l'Azienda risulti appaltatore e subappaltatore?

Se sì, i lavoratori sono muniti di apposita tessera di riconoscimento?

6.6 Ricettazione e riciclaggio

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

ATTIVITA' AZIENDALI A RISCHIO	CONTROLLI CCDAELATIVI
<ul style="list-style-type: none"> • Amministrazione • Commerciale • Finanza • Acquisti 	<ul style="list-style-type: none"> • Verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari, sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici - protesti, procedure concorsuali - o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; • Verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni. • Controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate. Verifiche sulla Tesoreria (rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità, ecc.); • Determinazione dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard

DESCRIZIONE

La presente Check list dispone a carico degli Esponenti Aziendali, dei Consulenti e dei Partner, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti del Gruppo nell'ambito dell'espletamento delle attività considerate a rischio, di attenersi ai seguenti principi generali di condotta.

RIS.

1. porre in essere, promuovere, collaborare, o dare cCdas a comportamenti tali da integrare le fattispecie rientranti tra i Reati ed Illeciti in materia di ricettazione e riciclaggio;

2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte possano potenzialmente diventarlo;

3. utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati in materia di ricettazione e riciclaggio.

4. In particolare, nell'espletamento delle attività connesse alle Aree a Rischio, è espressamente vietato ai Destinatari di porre in essere, collaborare o creare i presupposti per la realizzazione di comportamenti che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato e di illecito rientranti tra quelle considerate in materia di ricettazione e riciclaggio.

5. Nell'espletamento di tutte le operazioni attinenti alla gestione, oltre alle regole di cui al presente Modello, gli Esponenti aziendali sono tenuti in generale a conoscere e rispettare tutte le regole ed i principi contenuti nei seguenti documenti:

(i) il Codice etico;

(ii) il Regolamento interno per la gestione degli acquisti, vendite, delle forniture, dei contratti e di qualsivoglia operazione o transazione con terzi come trattate nella parte Generale del presente Modello e dalle procedure e protocolli interni aziendali. Ai Consulenti, Partner e Fornitori e parti terze deve essere resa nota l'adozione del Modello e del Codice etico da parte dell'Ente.

I Destinatari sono in particolare tenuti a provvedere – prima di compiere un'operazione ritenuta sospetta a trasmettere la segnalazione al ODV per ricevere indicazioni in merito. L'ODV per la formulazione di raccomandazioni e/o pareri potrà avvalersi della consulenza e del supporto dell'Organo Amministrativo. - Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

6) Relativamente alle operazioni indicate sopra al punto (ii) al fine di consentire al ODV di acquisire tutti gli elementi informativi necessari per l'espletamento del suo incarico, lo stesso dovrà essere tempestivamente informato dai responsabili delle funzioni relative:

a) dei termini delle transazioni in deroga

b) di eventuali delibere dell'Organo Amministrativo riguardanti operazioni in deroga;

c) di acquisti o vendite in deroga.

Le procedure aziendali che possono risultare rilevanti ai fini della prevenzione dei reati e degli illeciti in materia di ricettazione e riciclaggio possono essere aggiornate dai competenti organi aziendali, anche su proposta o segnalazione dell'ODV.

Sono ammesse, sotto la responsabilità di chi le attua, eventuali deroghe alle procedure previste dal Modello, nei soli casi di particolare urgenza nella formazione o nell'attuazione della decisione o in caso di impossibilità temporanea del rispetto delle procedure. In questi casi, è inviata immediata informazione all'ODV ed è sempre richiesta la successiva ratifica da parte del soggetto competente.

In particolare gli Organi di Governance hanno posto attenzione ai seguenti fattori:
 Vincoli di parentela tra Organi Sociali e P.A. Verifica delle parti terze nelle “ Liste”
 UIC Onorabilità e professionalità delle parti terze

Attendibilità commerciale (protesti, procedure concorsuali);

Persone politicamente esposte;

- Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio
- Identificazione di una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard.
- Identificazione di un organo/unità responsabile dell’esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità.
- Specifica previsione di regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio.
- Determinazione dei criteri di selezione, stipulazione ed esecuzione di accordi/joint-venture con altre imprese per la realizzazione di investimenti. Trasparenza e tracciabilità degli accordi/joint-venture con altre imprese per la realizzazione di investimenti.
- Verifica della congruità economica di eventuali investimenti effettuati in joint venture (rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di due diligence).

6.7 CHECK LIST PRIVACY E SICUREZZA DELLE INFORMAZIONI

Verifica	Evidenze
È evidente in azienda una sensibilità agli aspetti di riservatezza delle informazioni?	
Esiste un codice o un impegno formale della direzione al problema privacy?	
Le informazioni presenti in azienda sono state identificate in termini di criticità e di requisiti legali di riferimento?	
Il DPS (documento programmatico sulla sicurezza) è aggiornato (entro il 31 marzo di ogni anno)?	..
La documentazione (per esempio procedure) relativa alla privacy è debitamente approvata ?	
L’aggiornamento del DPS è inserito nella relazione annuale	

del bilancio?	
Vi è evidenza nel documento dei cambiamenti avvenuti (anche grafica)?	..
L'azienda ha subito sanzioni in materia di privacy?	
Sono presenti contenziosi in materia?	
È stato nominato un responsabile specifico della direzione per gestire questi aspetti?	
Vi sono evidenze di minacce alla riservatezza, disponibilità o integrità dei dati e delle informazioni?	..
L'azienda adotta o ha progetti di certificazione della riservatezza delle informazioni?	
L'azienda è seguita da consulenti esterni regolati da apposito contratto?
È stata verificata l'esigenza di notifica al garante ed in caso positivo è stata fatta?	
Sono esportati dati a rilevanza legale all'estero (UE o extra UE), se si è prevista una apposita procedura?

Controllo sulle attività operative

Verifica	Note
Sono state definite password (con identificazione utente) relativa per accesso a postazioni informatiche?	
Le password sono conservate in busta chiusa, con cambio semestrale o trimestrale per il trattamento dei dati sensibili?	..
È stata svolta formazione al personale sulle modalità di trattamento dei dati personali, sia in formato elettronico sia cartaceo, con particolare attenzione ai dati sensibili e	

verifica?	
Viene tenuto un registro dove annotare eventuali episodi che possono aver danneggiato i dati personali (per esempio virus)?	
Nell'attività di marketing tramite e-mail vi sono procedure o prassi specifiche (che richiama di consenso esplicito alla ricezione di e-mail promozionali)?	
Sono stati apposti i cartelli informativi per le eventuali videocamera che controllano un'area di passaggio pubblico e tenuta di una relazione sulle finalità dell'uso della stessa?	

Controllo documentale

Verifica	Note
Sono presenti le lettere di nomina degli incaricati di mansioni specifiche, come custode delle password, responsabile degli archivi, responsabile del salvataggio dei dati, responsabile del trattamento dei dati?	
Sono presenti le lettere di incarico al trattamento dei dati personali all'interno dell'azienda, in qualsiasi formato o supporto?	
Sono presenti le lettere di incarico al trattamento dei dati personali effettuati da terzi per conto dell'azienda (per esempio commercialisti, consulenti del lavoro, case di software, Medici del lavoro)?	
Sono presenti le informative ai clienti e fornitori?	
Sono presenti le informative ai dipendenti e collaboratori (firmate per accettazione)?	
È disponibile l'elenco formale degli incaricati al trattamento?	

I documenti sono disponibili per la verifica?	
---	--

Nota: il DPS (Documento Programmatico sulla Sicurezza) è un documento riepilogativo di quanto predisposto in materia di privacy, in cui vengono definite le persone coinvolte nelle operazioni di trattamento dei dati, le banche dati interessate ed analizzata la situazione ambientale, fisica ed organizzativa in cui i dati vengono trattati, i rischi rilevati e le misure consigliate per contrastarli.

Sono dati personali sensibili quei dati che rivelano l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, o l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; per esempio: buste paga, curriculum vitae, il registro delle presenze del personale e degli infortuni, i certificati medici, le schede sanitarie, le informative di insolubilità clienti e gli insoluti in genere, le dichiarazioni dei redditi di tipo personale.