



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL D. LGS. 8 GIUGNO 2001, N. 231

	Emissione	Agg. 1	Agg. 2
Copia n. 1	28/12/2016	02/05/2018	
Visto di verifica ed approvazione: Presidente			
Note:			

SOMMARIO

1. STRUTTURA DEL DOCUMENTO.....	5
2. IL DECRETO LEGISLATIVO N. 231/2001	6
2.1 INTRODUZIONE	6
2.2 FATTISPECIE DI REATO	6
2.3 LE VICENDE MODIFICATIVE DELL'ENTE	7
2.4 SANZIONI A CARICO DELL'ENTE	7
2.5 MODELLO DI ORGANIZZAZIONE E GESTIONE.....	8
3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO . 10	
3.1 FINALITA' DEL MODELLO.....	10
3.2 PRINCIPI ISPIRATORI DEL MODELLO	10
3.3 DESTINATARI DEL MODELLO	10
3.4 ADOZIONE DEL MODELLO E SUE REVISIONI.....	11
4. STRUTTURA ORGANIZZATIVA DELL'ENTE	13
4.1 PREMessa.....	13
4.2 ATTIVITA' ED ORGANIZZAZIONE DELL'ENTE	13
4.2.1 Scopi e funzioni	13
4.2.2 Struttura organizzativa	14
L'Ente è costituito dai seguenti organi:	14
4.3 CORPORATE GOVERNANCE	14
4.3.1 Codice Etico	14
4.3.2 Sistema di deleghe.....	14
4.3.3 Sistemi di Gestione, procedure e prassi	15
4.3.4 Sistemi ed attività di controllo e monitoraggio	15
5. LA COSTRUZIONE DEL MODELLO.....	16
5.1 METODI DI INDIVIDUAZIONE E CLASSIFICAZIONE DEI RISCHI	16
5.2 I REATI PREVISTI DALLA DGR 2120/2015 DELLA REGIONE VENETO	16
5.3 ESCLUSIONI - I REATI PERTINENTI PER L'ENTE	17
5.4 I PROCESSI SENSIBILI DELL'ENTE	17
6. L'ORGANISMO DI VIGILANZA	19
6.1 ISTITUZIONE DELL'ORGANISMO DI VIGILANZA.....	19
6.1.1 Struttura	19
6.1.2 Componenti e durata in carica	19
6.2 FUNZIONI, POTERI ED ATTIVITA' DELL'ORGANISMO DI VIGILANZA.....	20
6.3 REPORTING E SEGNALAZIONI DELL'ORGANISMO DI VIGILANZA	21
6.4 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA	22

7. INFORMAZIONE E FORMAZIONE	23
7.1 DIPENDENTI INTERNI	23
7.2 COLLABORATORI ESTERNI	23
8. SISTEMA SANZIONATORIO	24
8.1 PRINCIPI GENERALI.....	24
9. PARTE SPECIALE A - I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE ED I REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA	26
9.1 FATTISPECIE DI REATO	26
9.1.1 Esclusioni.....	29
9.1.2 Individuazione dei processi sensibili	29
9.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO	29
9.2.1 Richiesta finanziamenti e contributi pubblici	30
9.2.2 Gestione rapporti con gli enti pubblici per rilascio autorizzazioni e/o obblighi di informativa.....	31
9.2.3 Verifiche e ispezioni svolte da soggetti esterni	32
9.2.4 Rapporti con l'Autorità Giudiziaria	33
9.2.5 Acquisti di beni e servizi	33
9.2.6 Gestione regali e omaggi	34
9.2.7 Gestione del personale	35
9.2.8 Principi generali di comportamento e di attuazione dei processi nelle aree di attività a rischio	35
9.3 FLUSSI INFORMATIVI VERSO L'ODV	36
10. PARTE SPECIALE B - I DELITTI INFORMATICI ED I REATI CON VIOLAZIONE DEI DIRITTI D'AUTORE	38
10.1 FATTISPECIE DI REATO	38
10.1.1 Esclusioni.....	43
10.1.2 Individuazione dei processi sensibili.....	43
10.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO	44
10.2.1 Utilizzo del sistema informatico e del sito web	44
10.2.2 Utilizzo della firma digitale	45
10.2.3 Utilizzo di software e banche dati	45
10.3 FLUSSI INFORMATIVI VERSO L'ODV	45
11. PARTE SPECIALE C - I REATI SOCIETARI	47
11.1 FATTISPECIE DI REATO	47
11.1.1 Esclusioni.....	50
11.1.2 Individuazione dei processi sensibili.....	51
11.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO	51
11.3 FLUSSI INFORMATIVI VERSO L'ODV	53
12. PARTE SPECIALE D - I REATI DI RICETTAZIONE E RICICLAGGIO.....	55
12.1 FATTISPECIE DI REATO.....	55
12.1.1 Esclusioni.....	57
12.1.2 Individuazione dei processi sensibili.....	57
12.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO	57

12.3 FLUSSI INFORMATIVI VERSO L'ODV	58
13. PARTE SPECIALE E - I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO	60
13.1 FATTISPECIE DI REATO	60
13.1.1 Esclusioni	60
13.1.2 Individuazione dei processi sensibili.....	60
13.2 PRINCIPI DI COMPORTAMENTO NELL'AMBITO DELLE ATTIVITÀ A RISCHIO - ELEMENTI ATTUATIVI DEL MODELLO	60
13.3 INFORMATIVI VERSO L'ODV	61

1. STRUTTURA DEL DOCUMENTO

L'entrata in vigore del D.Lgs. 231/01 ha introdotto nel nostro ordinamento la responsabilità amministrativa degli Enti, quale conseguenza della commissione di determinati reati da parte di Soggetti "Apicali" o "Sottoposti", sempre che tali fatti siano commessi nell'interesse o a vantaggio dell'ente stesso.

- L'inosservanza di tale disciplina può comportare per l'ente sanzioni che possono arrivare fino all'interdizione dall'esercizio dell'attività. Tuttavia, qualora l'organo dirigente dell'ente provi di aver adottato ed efficacemente attuato, prima della commissione del reato, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi, l'ente non risponde per la responsabilità amministrativa, indipendentemente dal riconoscimento della responsabilità penale della persona che ha commesso il reato.

L'Ente, facendo anche riferimento alle linee guida emanate da Confindustria e alle *best practice* di controllo interno, ha provveduto, pertanto, ad elaborare il presente Modello.

Il Modello si compone delle seguenti Parti:

- Parte Generale. Dopo *un excursus* esplicativo del D.Lgs 231/01 a vantaggio di tutti i soggetti cui verrà divulgato il MOG, nella Parte Generale viene descritto il profilo organizzativo dell'Ente, tra cui i meccanismi di *governance* adottati, la metodologia seguita nella redazione del Modello, l'Organismo di Vigilanza, il Sistema Sanzionatorio previsto e la Formazione sul Modello.
- Parte Speciale A - "I reati contro la pubblica amministrazione e l'amministrazione della giustizia"
- Parte Speciale B - "I delitti informatici e il diritto d'autore"
- Parte Speciale C - "I reati societari"
- Parte Speciale D - I reati di ricettazione, riciclaggio o impiego di denaro o beni di illecita provenienza
- Parte Speciale E - "I reati nella sicurezza sul lavoro"

Ciascuna parte speciale è a sua volta suddivisa in:

- Individuazione delle singole fattispecie di reato
- L'individuazione delle attività a rischio/processi sensibili dell'Ente, eventuali esclusioni.
- L'analisi dei rischi e principi di comportamento nell'ambito dei processi sensibili.
- L'indicazione dei compiti dell'OdV in relazione a detta parte.

Ciascun destinatario del Modello è tenuto alla conoscenza ed osservanza dei principi e delle regole dello stesso.

L'Ente, pertanto, renderà note le finalità del Modello ed i contenuti del Codice Etico attraverso i mezzi e le forme che riterrà più adeguate, tramite attività di formazione ed iniziative specifiche.

2. IL DECRETO LEGISLATIVO N. 231/2001

2.1 INTRODUZIONE

In data 4 luglio 2001 è entrato in vigore il Decreto Legislativo 8 giugno 2001 n. 231, avente ad oggetto la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica", il quale ha introdotto nell'ordinamento giuridico italiano la responsabilità degli Enti per gli illeciti amministrativi derivanti da reati commessi nell'interesse o a vantaggio dei medesimi Enti.

Il Decreto si applica nel settore privato alle Società, associazioni ed enti con personalità giuridica, mentre nel settore pubblico soltanto agli enti pubblici economici (con esplicita esclusione dello Stato, degli enti pubblici territoriali, degli enti pubblici non economici e degli enti che svolgono funzioni di rilievo costituzionale).

Il Decreto ha portata complessa ed innovativa, in quanto, alla responsabilità penale della persona fisica che ha commesso un reato, aggiunge quella dell'Ente nell'interesse del quale o a vantaggio del quale il reato stesso è stato perpetrato.

Infatti, l'art. 5 del Decreto stabilisce che l'Ente è chiamato a rispondere ogniqualvolta determinati reati (specificati nel Decreto), detti reati-presupposto, siano stati commessi *"nel suo interesse o a suo vantaggio"*, da parte dei seguenti soggetti:

- a) Persone che rivestono funzioni di rappresentanza, amministrazione o direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano anche di fatto la gestione e il controllo dello stesso (c.d. Soggetti Apicali o in Posizione Apicale);
- b) Persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla precedente lettera a).

La responsabilità dell'Ente è definita dal legislatore di tipo amministrativo, pur se disciplinata all'interno del procedimento penale, e si caratterizza, inoltre, per essere titolo autonomo di responsabilità rispetto a quella della persona fisica che commette il reato. Infatti, ai sensi dell'articolo 8 del Decreto, l'Ente può essere dichiarato responsabile anche se l'autore materiale del reato non sia imputabile o non sia stato individuato ed anche se il reato sia estinto per cause diverse dall'amnistia. In base al medesimo principio, ogni eventuale imputazione all'Ente di responsabilità derivante dalla commissione del reato non vale ad escludere la responsabilità penale personale di chi ha posto in essere la condotta criminosa.

2.2 FATTISPECIE DI REATO

La responsabilità dell'Ente non è riferibile a qualsiasi reato, ma è circoscritta alle fattispecie penali indicate espressamente dal Decreto, che prevede, alla data di approvazione del presente Modello:

- art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico;
- art. 24 bis - Reati informatici e di trattamento illecito dei dati
- art. 24 ter - Delitti di criminalità organizzata;
- art. 25 - Concussione, induzione indebita a dare o promettere utilità e corruzione;
- art. 25 bis - Falsità in monete, in carte di pubblico credito e in valori di bollo;
- art. 25 bis 1 - Delitti contro l'industria e il commercio;
- art. 25 ter - Reati societari;
- art. 25 quater - Delitti con finalità di terrorismo o di eversione dell'ordine democratico;
- art. 25 quater 1 - Pratiche di mutilazione degli organi genitali femminili;

- art. 25 quinquies - Delitti contro la personalità individuale;
- art. 25 sexies - Abusi di mercato;
- art. 25 septies - Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- art. 25 octies - Reati di riciclaggio, ricettazione e di impiego di denaro, beni o utilità di provenienza illecita;
- art. 25 novies - Delitti in materia di violazione del diritto d'autore;
- art. 25 decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- art. 25 undecies - Reati ambientali;
- art. 25 duodecies - Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare.

2.3 LE VICENDE MODIFICATIVE DELL'ENTE

Il principio fondamentale, che informa anche l'intera materia della responsabilità dell'ente, stabilisce che «dell'obbligazione per il pagamento della sanzione pecuniaria» inflitta all'ente «risponde soltanto l'ente, con il suo patrimonio o il fondo comune».

Alle sanzioni pecuniarie inflitte all'ente si applicano, in caso di trasformazione, i principi delle leggi civili sulla responsabilità per i debiti dell'ente originario.

Per le sanzioni interdittive si è stabilito, invece, che esse rimangano a carico dell'ente in cui sia rimasto (o sia confluito) il ramo di attività nell'ambito del quale è stato commesso il reato, salva la facoltà per l'ente risultante dalla trasformazione di ottenere la conversione della sanzione interdittiva in sanzione pecuniaria.

Il Decreto sancisce la regola che, nel caso di «trasformazione dell'ente, resta ferma la responsabilità per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto».

Nel caso di operazioni di fusioni e/o di scissioni, il Decreto prevede che l'ente risultante dalla fusione, anche per incorporazione, «risponde dei reati dei quali erano responsabili gli enti partecipanti alla fusione». Al subentrare dell'ente risultante dalla fusione nei rapporti giuridici degli enti fusi consegue, dunque, un trasferimento della responsabilità in capo all'ente scaturito dalla fusione.

Tuttavia, se la fusione è intervenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il giudice deve tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

Gli enti collettivi beneficiari di un'operazione di scissione, ai quali sia pervenuto il patrimonio (in tutto o in parte) dell'Ente scissa sono solidalmente obbligati al pagamento delle sanzioni pecuniarie dovute dall'ente scisso per reati anteriori alla scissione. L'obbligo è limitato al valore del patrimonio trasferito.

Nel caso di un'operazione di cessione e/o di conferimento dell'azienda nell'ambito della quale è stato commesso il reato, il cessionario è solidalmente obbligato con l'ente cedente al pagamento della sanzione pecuniaria, nei limiti del valore dell'azienda ceduta e salvo il beneficio della preventiva escussione dell'ente cedente.

La responsabilità del cessionario - oltre che limitata al valore dell'azienda oggetto di cessione (o di conferimento) - è, peraltro, limitata alle sanzioni pecuniarie che risultano dai libri contabili obbligatori, ovvero dovute per illeciti amministrativi di cui il cessionario era comunque a conoscenza.

2.4 SANZIONI A CARICO DELL'ENTE

Le sanzioni previste a carico dell'Ente, in conseguenza della commissione o tentata commissione dei reati presupposto, sono:

- **sanzione pecuniaria**, che può variare a seconda della gravità del reato, del grado di responsabilità dell'ente, dell'attività svolta per eliminare le conseguenze del fatto e attenuarne le conseguenze o per prevenire la commissione di altri

illeciti e che tiene conto delle condizioni economiche e patrimoniali dell'ente, e dello scopo di assicurare l'efficacia della sanzione. In caso di condanna dell'ente, la sanzione pecuniaria è sempre applicata;

- **sanzioni interdittive**, quali l'interdizione dall'esercizio dell'attività, la sospensione o revoca di licenze o concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione o revoca di finanziamenti e contributi e il divieto di pubblicizzare beni e servizi.

Le sanzioni interdittive sono irrogate, congiuntamente a quella pecuniaria, solo se espressamente previste per quella fattispecie di reato e soltanto quando ricorre almeno una di queste due condizioni:

- 1) l'Ente ha già commesso in precedenza un illecito da reato;
- 2) l'Ente ha tratto dal reato un profitto di elevata entità.

La durata delle sanzioni interdittive è normalmente temporanea, in un intervallo che va da tre mesi a due anni.

Solo in casi particolarmente gravi, alcune sanzioni interdittive possono essere disposte in via definitiva. Le sanzioni interdittive possono essere applicate anche in via cautelare, su richiesta del Pubblico Ministero, qualora sussistano gravi indizi della responsabilità dell'ente e vi siano fondati e specifici elementi tali da far ritenere il concreto pericolo che vengano commessi illeciti dello stesso tipo di quello già commesso.

- **confisca** (e sequestro preventivo in sede cautelare) del profitto e del prezzo del reato, anche in forma per equivalente;
- **pubblicazione della sentenza** (che può essere disposta dal giudice quando, nei confronti dell'ente, viene applicata una sanzione interdittiva).

2.5 MODELLO DI ORGANIZZAZIONE E GESTIONE

Il Decreto introduce una particolare forma di esonero dalla responsabilità in oggetto qualora l'Ente dimostri:

- di aver adottato ed efficacemente attuato attraverso l'organo dirigente, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- di aver affidato a un organismo - Organismo di Vigilanza - dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curare il loro aggiornamento;
- che le persone, che hanno commesso il reato - nel caso trattasi di soggetti Apicali o equiparati - abbiano agito eludendo fraudolentemente i suddetti modelli di organizzazione e di gestione;
- che non vi sia omessa o insufficiente vigilanza da parte dell'organismo di Vigilanza.

Il Decreto prevede, inoltre, che, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di organizzazione, gestione e controllo debbano rispondere alle seguenti esigenze:

- individuare le aree a rischio di commissione dei reati previsti dal Decreto;
- predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- prevedere modalità di individuazione e di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello di organizzazione e controllo;
- configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione e controllo.

Il Decreto dispone che il modello di organizzazione e controllo possa essere adottato, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare (entro 30 giorni) osservazioni sulla idoneità dei modelli a prevenire i reati.

E', infine, previsto che negli Enti di piccole dimensioni il compito di vigilanza possa essere svolto direttamente dall'organo dirigente, e nelle società di Capitali dal Collegio Sindacale, dal Consiglio di Sorveglianza o dal Comitato per il Controllo e la Gestione.

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

3.1 FINALITA' DEL MODELLO

Il presente Modello è stato realizzato al fine di raggiungere molteplici obiettivi:

- disporre di uno strumento di analisi delle aree a rischio per la commissione dei reati previsti dal D.lgs. 231/01;
- riunire in modo organico ed organizzato l'insieme di procedure, regole, prassi e sistemi gestionali già in atto in azienda, implementare quelli che si sono individuati come ulteriormente necessari, il tutto con lo scopo di regolare i processi sensibili nel rispetto dei principi del Codice Etico;
- diffondere a tutti i livelli e presso tutti i portatori di interesse l'impegno dell'Ente nel perseguimento degli obiettivi di responsabilità sociale fissati all'interno del Codice Etico, e nella censura di tutti i comportamenti non conformi a quanto ivi prescritto;
- dare atto dell'impegno dell'Ente alla costante ed efficace prevenzione dei reati elencati all'interno del D. Lgs. 231/01, non solo ai fini esimenti previsti dallo stesso Decreto, ma per una sempre più attenta valorizzazione dei principi di responsabilità sociale;
- stabilire un chiaro ed efficace sistema sanzionatorio, a tutti i livelli, che possa dare un contributo alla prevenzione dei reati, oltre che rappresentare uno strumento essenziale di tutela per l'Ente nei confronti di eventuali dipendenti/amministratori non allineati alle norme di condotta stabilite dall'azienda.

3.2 PRINCIPI ISPIRATORI DEL MODELLO

I principi fondamentali sulla base delle quali è costruito il Modello, sono:

- la mappatura delle attività sensibili;
- l'identificazione delle operazioni significative nell'ambito delle attività sensibili ove sia presente un possibile rischio di commissione di reati presupposto;
- l'applicazione e il rispetto del principio di segregazione delle funzioni, e la creazione di un efficace sistema di deleghe;
- l'attribuzione di poteri coerenti con le responsabilità organizzative;
- l'attribuzione all'Organismo di Vigilanza di specifici compiti di controllo sull'efficace e corretto funzionamento del Modello;
- la diffusione e il coinvolgimento di tutti i livelli aziendali nell'attuazione di regole comportamentali, procedure e politiche aziendali conformi ai principi stabiliti nel Modello;
- un efficace sistema sanzionatorio.

3.3 DESTINATARI DEL MODELLO

Il presente modello, realizzato a favore di tutti i portatori di interesse dell'Ente, si rivolge espressamente a:

- gli amministratori e coloro che svolgono, anche di fatto, funzioni di rappresentanza, gestione, amministrazione, direzione o controllo nell'Ente;
- personale dipendente, a tutti i livelli;
- collaboratori, consulenti, fornitori dell'Ente, soggetti terzi che vengano in rapporto con l'Ente.

L'Ente comunica il presente Modello ai Destinatari attraverso modalità idonee ad assicurarne l'effettiva conoscenza da parte di tutti i soggetti interessati. I Destinatari del Modello sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in

adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con l'Ente.

La stessa condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello e del Codice Etico, tanto più se tale comportamento sia realizzato nell'interesse aziendale, ovvero con l'intenzione di arrecare un vantaggio all'Ente.

Con riferimento, invece, a soggetti diversi rispetto ai Destinatari del Modello, al fine di ottenere la più ampia osservanza dello stesso e di attuare il relativo sistema sanzionatorio, l'Ente determina i casi in cui richiedere l'applicazione dei principi di cui al Modello e al proprio Codice Etico anche da parte di soggetti esterni diversi dai Destinatari. A tal fine, i contratti che regolano i rapporti con tali soggetti prevedranno apposite clausole (incluse clausole risolutive espresse) che indichino chiaramente le responsabilità e le conseguenze dovute al mancato rispetto del Codice Etico dell'Ente, opportunamente comunicato, e dei principi ispiratori del presente Modello. L'Ente valuterà i casi più rilevanti nei quali richiedere ai terzi l'obbligo di ottemperare alle richieste di informazioni o di esibizione di documenti formulate dall'Organismo di Vigilanza dell'Ente e di segnalare direttamente all'Organismo di Vigilanza dell'Ente le violazioni del Modello, dei principi di cui al Codice Etico o delle procedure stabilite per la loro attuazione.

3.4 ADOZIONE DEL MODELLO E SUE REVISIONI

Il Consiglio di Amministrazione dell'Ente adotta il presente Modello di Organizzazione e Gestione mediante apposita delibera; il Modello è, quindi, un documento ufficiale dell'Ente e come tale deve essere noto e rispettato a tutti i livelli interni.

Tramite l'adozione del Modello, quindi, l'Ente intende assicurarsi che dai propri amministratori, dipendenti e collaboratori a qualsiasi titolo, non siano commesse fattispecie di reato che possano non solo screditare l'immagine dell'Ente stessa, ma anche comportare l'applicazione di una delle sanzioni pecuniarie e/o interdittive che il Decreto prevede nel caso in cui tali reati siano posti in essere a vantaggio o nell'interesse dell'Ente.

Il presente Modello può essere modificato o integrato esclusivamente con successiva delibera del Consiglio, previa proposta e/o consultazione formale con l'Organismo di Vigilanza. Quest'ultimo provvede tempestivamente a segnalare al Consiglio ogni fatto o circostanza riscontrati nella propria opera di vigilanza che comportino la necessità di revisione dei contenuti del Modello, proponendone anche le eventuali modifiche.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PARTE GENERALE

4. STRUTTURA ORGANIZZATIVA DELL'ENTE

4.1 PREMESSA

TER SERVIZI CONFCOMMERCIO VENEZIA S.r.l. è società di fornitura di servizi di formazione e di orientamento al lavoro e professionale per la provincia di Venezia, le cui quote sono detenute al 20% da Ascom Servizi Portogruaro S.r.l., al 20% da Ascom Servizi S.r.l. del mandamento di San Donà di Piave e al 60% dall'Unione delle Imprese, delle Attività Professionali e del Lavoro.

È ente accreditato dalla Regione Veneto in diversi ambiti:

- 1) Accreditalamento ai servizi al lavoro per le persone fisiche
- 2) Accreditalamento alla formazione continua e superiore per le Aziende

L'accreditalamento ai servizi al lavoro comporta la possibilità di svolgere attività di assistenza nella ricerca attiva di un'occupazione o nel ricollocamento su istanza di un singolo soggetto. Tale attività può comportare anche l'organizzazione di un tirocinio per il lavoratore, verificato da un tutor dell'azienda interessata.

L'accreditalamento alla formazione continua e superiore per le Aziende permette di organizzare corsi finanziati da fondi regionali (FSE) o interprofessionali (Fondo Forte) o dagli Enti Bilaterali del Turismo e del Terziario.

La società ha n. 10 dipendenti.

La sede legale è in Venezia, Viale Ancona 9, frazione di Mestre.

Sussistono, poi, due unità locali: Unità Locale n. VE/2 in Portogruaro (VE), Borgo S. Agnese 93 e Unità Locale n. VE/3 in San Donà di Piave (VE), Via Como n. 5.

4.2 ATTIVITA' ED ORGANIZZAZIONE DELL'ENTE

4.2.1 Scopi e funzioni

TER SERVIZI S.R.L. ha per oggetto sociale la fornitura, sotto qualsiasi forma, di beni e servizi che siano reputati utili, dall'organo amministrativo, alla gestione e sviluppo delle imprese e delle economie in genere. Pertanto la società, richiedendo le autorizzazioni previste dalla legislazione se del caso, potrà: produrre e somministrare servizi sia a carattere temporaneo che continuativo riservandosi o meno le proprietà o altri diritti; acquisire servizi da terzi sia per uso interno che per la rivendita, distribuzione o somministrazione in proprietà totale o parziale e riconoscendo o meno diritti continuativi al cessionario, sia in uso gratuito che oneroso; acquisire beni materiali sia per uso interno che per la rivendita, in proprietà, comodato, locazione anche finanziaria, con o senza rappresentanza e di commissionaria; svolgere attività di assistenza tecnica e finanziaria; studiare, elaborare, gestire progetti ed iniziative sia che queste siano interamente gravate dal rischio imprenditoriale sia che possano accedere a forme di sostegno economico previsto dalle leggi nazionali e regionali e da provvedimenti comunitari e degli enti locali, avanzando le relative richieste ecc.

In particolare, ricomprese nell'oggetto sociale sono la progettazione, l'organizzazione e la realizzazione di programmi e di studi per i percorsi formativi e preformativi; la realizzazione, conduzione e gestione di corsi di formazione compresi quelli rivolti alla

qualificazione e riqualificazione professionale e all'aggiornamento tecnico degli operatori economici e loro addetti nonché per coloro che intendono entrare nel mondo del lavoro; la ricerca del personale per conto terzi; l'organizzazione e la realizzazione di servizi di orientamento al lavoro e professionale e per favorire l'incontro tra domanda e offerta di lavoro.

4.2.2 Struttura organizzativa

L'Ente è costituito dai seguenti organi:

- Assemblea dei soci
- Consiglio di Amministrazione

All'interno del Consiglio di Amministrazione oltre al Presidente, rappresentante dell'impresa, è stato nominato un Consigliere Delegato, con potere di firma degli atti di ordinaria amministrazione, compresi i rapporti bancari e quant'altro previsto dallo Statuto per la carica di Presidente e dal Codice civile.

Esiste un Responsabile del Coordinamento del personale, collaboratore esterno, ~~che è anche responsabile commerciale~~, come risulta da organigramma allegato.

Ciascun organo dell'Ente è previsto e disciplinato dallo Statuto agli art. 12 e ss. dove sono definite funzioni, competenze e modalità di nomina/elezione.

A questi organi va ad aggiungersi l'Organismo di Vigilanza, espressamente previsto dal D. Lgs. 231/01.

Ter Servizi, per l'esercizio della propria attività, in particolare per l'organizzazione di corsi di formazione e di aggiornamento professionale, dispone della sede legale sopra indicata nonché delle due unità locali.

4.3 CORPORATE GOVERNANCE

4.3.1 Codice Etico

Ter Servizi si è dotata di un Codice Etico che rappresenta il sunto di tutti i principi di responsabilità sociale che la società si è data e che la stessa richiede nei propri collaboratori e nei terzi con cui essa interagisce.

Al documento viene data massima diffusione, con pubblicazione anche sul sito web dell'Ente, affinché possa essere conosciuto da chiunque sia in rapporto con l'Ente stesso.

Ter Servizi riconosce come destinatari dei principi del proprio agire i seguenti soggetti:

- I soci;
- I lavoratori dipendenti, i collaboratori esterni, i consulenti;
- La comunità locale, la cittadinanza, i vicini (siano essi privati o aziende o Enti);
- L'ambiente esterno, in particolare il territorio confinante con la propria sede;
- I fornitori dell'Ente, siano essi di materiali o di servizi;
- Lo Stato e le sue istituzioni rappresentative, la Pubblica Amministrazione, le Autorità.

I principi contenuti nel Codice Etico sono emanazione del Consiglio di Amministrazione, vengono resi noti pubblicamente a tutte le parti interessate mediante comunicazioni mirate o generali, devono essere sempre rispettati a tutti i livelli.

4.3.2 Sistema di deleghe

Ter Servizi si è dotata – anche nell’ambito della segregazione delle funzioni e di un miglioramento organizzativo – di un organigramma/fuzionigramma che viene allegato al Modello.

Il Consiglio di Amministrazione, ha poi ritenuto di implementare un sistema di deleghe per quanto riguarda i seguenti aspetti specifici:

- Amministratore Delegato con gli stessi poteri previsti da Statuto per il Presidente del CdA

Il Consiglio di Amministrazione ha poi nominato, al proprio interno, un Datore di lavoro per la Sicurezza ai sensi dell’art. 2 del D. Lgs. 81/08.

4.3.3 Sistemi di Gestione, procedure e prassi

L’Ente che, ha già alcune prassi interne consolidate, nonché dei procedimenti formalizzati nella struttura del Sistema ISO 9001 anche se formalmente non certificato, si è dotato di un sistema CRM Open Source “V-TIGER”.

Gli aspetti principali dell’attività sono disciplinati da alcuni regolamenti quali:

- Regolamento docenti
- Regolamento per l’uso dei sistemi informatici;
- Il Regolamento per il personale (anche per l’utilizzo dei dati personali)

Nella parte speciale del presente modello sono espressamente richiamate le procedure in essere o esistenti o, comunque, utilizzate alla data di approvazione del Modello, nonché le prassi in uso. Queste ultime potranno essere formalizzate in procedure specifiche che, una volta approvate, verranno conseguentemente implementate e richiamate nel presente Modello.

Qualora si verificasse la necessità dell’aggiornamento di una procedura, il soggetto proponente la modifica dovrà farne richiesta al Coordinatore che, consultatosi con il Consiglio di Amministrazione, ne curerà la riedizione. La nuova procedura verrà successivamente approvata dal Consiglio di Amministrazione e resa nota a tutti gli interessati tramite la circolarizzazione, l’informazione e la formazione sulla stessa.

Vi sono poi alcune prassi consolidate, non formalizzate all’interno del Sistema, che derivano dall’applicazione dei regolamenti regionali e/o dei fondi interprofessionali, nonché dall’applicazione dei principi del Codice Etico, e sono quindi note e rispettate dai dipendenti amministrativi e tecnici nello svolgimento delle loro mansioni.

4.3.4 Sistemi ed attività di controllo e monitoraggio

Le attività di controllo e monitoraggio sulla corretta applicazione delle procedure esistenti e delle norme interne è affidata, innanzitutto, al Consiglio di Amministrazione e al Coordinatore del personale che, il quale vigila anche sull’operato di tutti i dipendenti. L’Organismo di Vigilanza – sia nei controlli periodici che a campione – provvede a verificare l’attuazione del Sistema 231, con l’apporto anche di tutti i soggetti interessati che hanno l’obbligo di informare l’Organo di Vigilanza di ogni “non conformità” o “comportamento difforme”.

5. LA COSTRUZIONE DEL MODELLO

5.1 METODI DI INDIVIDUAZIONE E CLASSIFICAZIONE DEI RISCHI

L'Ente ritiene che l'analisi dei rischi rappresenti la base fondamentale del Modello di Organizzazione e Gestione, in quanto necessaria ad evidenziare le aree ed i processi sensibili alla commissione dei reati ricompresi nel D. Lgs. 231/01, ed essenziale per determinare l'entità dei rischi e la bontà delle misure di prevenzione attuate dall'azienda. Per quanto sopra, l'Ente ha dato incarico ad un gruppo di professionisti esperti nelle materie in esame, di realizzare un'approfondita e dettagliata analisi dei rischi e conseguente loro stima, tenendo in considerazione:

- Le caratteristiche dell'Ente, l'ambito di attività e l'organizzazione interna dello stesso;
- Il livello di diffusione ed accettazione dei principi contenuti nel Codice Etico;
- Le prassi consolidate e le procedure esistenti per la regolamentazione dei processi associativi;
- I dati storici rilevanti.

Il metodo adottato per l'analisi e stima dei rischi ha comportato:

- Una serie di incontri presso la sede di Ter Servizi, con il coinvolgimento diretto del Coordinatore e del Responsabile commerciale e delle figure operative interessate dall'analisi in corso.
- La mappatura dei processi e delle aree sensibili.
- L'esame dettagliato di ogni singolo reato, sulla base delle interpretazioni giurisprudenziali e della dottrina, e la valutazione delle possibilità di commissione dello stesso all'interno dell'Ente.
- L'esame e la raccolta delle procedure e dei presidi di controllo esistenti, per le aree ed i processi a rischio.
- La verifica dei livelli di diffusione e conoscenza dei principi ispiratori del Modello.
- La proposta di procedure supplementari, o di modifiche alle esistenti, per aumentare i livelli di sicurezza.

All'interno di ogni singola parte speciale del presente Modello, sono riportate le risultanze delle verifiche svolte, con l'indicazione dei sistemi di prevenzione - presidi generali e speciali - in essere all'interno dell'Ente.

5.2 I REATI PREVISTI DALLA DGR 2120/2015 DELLA REGIONE VENETO

Al fine del presente Modello, che viene adottato anche ai sensi e per gli effetti della DGR 2120/2015 "Aggiornamento delle disposizioni regionali in materia di accreditamento degli Organismi di formazione ai sensi della L.R. 19/2002 e s.m.i. requisito 1.1.1. adozione modello D.lgs 231/2001 linee guida" sono stati considerati non solo alcuni tra i reati previsti dal D.Lgs. 231/01, ma anche quanto espressamente indicato nell'allegato A al D.D.R. 192 del 30 maggio 2016.

In particolare si sono analizzati

- a) reati contro la Pubblica Amministrazione;
- b) reati societari
- c) delitti informatici;
- d) trattamento illecito dei dati;
- e) sicurezza sul posto di lavoro;
- f) reati contro la personalità individuale.

5.3 ESCLUSIONI - I REATI PERTINENTI PER L'ENTE

Dall'analisi dei rischi effettuata, è emerso che alcune categorie di illeciti non sono ipotizzabili a carico dell'Ente, come i delitti contro la personalità individuale, o che il rischio di verificazione di alcune fattispecie criminose è, al momento, basso, sia alla luce dell'attività svolta e delle caratteristiche della Società, che dell'organizzazione aziendale.

Oltre alle fattispecie indicate dalla Regione Veneto, si evidenzia che anche altri reati contemplati dal D.Lgs. 231/2001 non appaiono concretamente configurabili nella realtà societaria, tra cui, a titolo esemplificativo, i delitti contro l'industria e il commercio.

Di conseguenza, i reati analizzati che sono stati considerati rilevanti per l'Ente sono i seguenti:

- reati contro la Pubblica Amministrazione;
- reati societari;
- delitti informatici, violazione del diritto d'autore e trattamento illecito dei dati;
- reati di ricettazione e riciclaggio;
- reati in materia di sicurezza sul posto di lavoro.

5.4 I PROCESSI SENSIBILI DELL'ENTE

Dall'analisi dei rischi condotta nell'ambito dell'attività esercitata ai fini del D.Lgs. 231/2001, è emerso che i Processi Sensibili dell'Ente riguardano allo stato principalmente:

- La richiesta di finanziamenti/contributi pubblici (corruzione, induzione indebita a dare o promettere utilità, indebita percezione di erogazioni, malversazione e in via subordinata truffa a danno dello Stato)
- La gestione dei rapporti con gli enti pubblici per il rilascio di autorizzazioni e/o gli obblighi di informativa (corruzione, concussione, induzione indebita a dare o promettere utilità e truffa a danno della Stato)
- I rapporti con l'Autorità Giudiziaria (concussione, corruzione, induzione indebita a dare o promettere utilità, induzione a non rendere dichiarazioni o rendere dichiarazioni mendaci all'Autorità giudiziaria)
- Le verifiche e le ispezioni svolte da soggetti esterni (concussione, corruzione, anche tra privati, induzione indebita a dare o promettere utilità)
- L'acquisto di beni e servizi (reati di corruzione, anche tra privati, induzione indebita a dare o promettere utilità; ricettazione riciclaggio e autoriciclaggio);
- La gestione di regali e omaggi (concussione, corruzione, anche tra privati, o induzione indebita a dare o promettere utilità)
- La gestione della liquidità e dei pagamenti (rilevante per molte fattispecie criminose, tra i quali, i reati contro la Pubblica Amministrazione, corruzione tra privati, ricettazione, riciclaggio e autoriciclaggio ecc.); il processo di definizione del bilancio (reati societari, ricettazione riciclaggio o autoriciclaggio)
- La gestione del personale (concussione, reati di corruzione, anche tra privati, induzione indebita a dare o promettere utilità)
- La gestione del servizio di fornitura della formazione/il rapporto con i fornitori (reati di corruzione, induzione indebita a dare o promettere utilità)
- L'utilizzo del sistema informatico aziendale e del sito web; l'utilizzo della firma digitale; l'utilizzo di software e banche dati; il trattamento dei dati personali (principalmente reati informatici, ma tali attività interessano trasversalmente molte delle fattispecie criminose analizzate)

Le attività che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001, sono elencate in dettaglio nelle rispettive Parti Speciali.

Seguendo l'evoluzione legislativa o quella dell'attività sociale, l'Organismo di Vigilanza ha il potere di individuare eventuali ulteriori attività a rischio che potranno essere ricomprese nell'elenco dei Processi Sensibili, all'interno della costante opera di aggiornamento ed implementazione del Modello.

6. L'ORGANISMO DI VIGILANZA

6.1 ISTITUZIONE DELL'ORGANISMO DI VIGILANZA

Il compito di vigilare continuativamente sull'efficace funzionamento e sull'osservanza del Modello, nonché di proporre l'aggiornamento, è affidato ad un organismo dell'Ente dotato di autonomia ed indipendenza, anche economica, nell'esercizio delle sue funzioni, nonché di adeguata professionalità in materia di controllo dei rischi pertinenti per le attività dell'azienda.

I componenti dell'Organismo di Vigilanza devono, quindi, possedere requisiti soggettivi che garantiscano l'autonomia, l'indipendenza, la professionalità e l'onorabilità dell'organismo stesso nell'espletamento delle sue attività.

La caratteristica dell'autonomia di poteri di iniziativa e di controllo comporta che tale Organismo debba essere:

- in una posizione di indipendenza rispetto a coloro su cui deve effettuare la vigilanza;
- privo di compiti operativi;
- dotato di autonomia finanziaria.

6.1.1 Struttura

In considerazione delle previsioni che precedono, l'Organismo di Vigilanza non può essere individuato nel Consiglio di Amministrazione, che è organo esecutivo con poteri gestionali ed è direttamente coinvolto nella gestione operativa della società.

Il Consiglio di Amministrazione ha ritenuto, perciò, che la composizione dell'Organismo di Vigilanza dell'Ente che meglio risponde ai requisiti indicati dal Decreto sia la seguente:

- almeno un soggetto, non facente parte dell'Ente dotato di un elevato livello di onorabilità e professionalità, scelto preferibilmente all'interno delle seguenti categorie professionali:
 - revisori contabili;
 - commercialisti,
 - avvocati;
 - consulenti del lavoro;
 - esperti in materia di sicurezza e ambiente
 - docenti universitari o comunque esperti in materia del D. Lgs. 231/01;
- almeno un soggetto, interno all'organizzazione, possibilmente già internal-auditor per i sistemi di gestione, o il responsabile stesso, in qualità di membro puramente consultivo, al fine di una migliore conoscenza della struttura e di costante flusso comunicativo verso l'Organismo di Vigilanza.

6.1.2 Componenti e durata in carica

Il Consiglio di Amministrazione provvede alla nomina dell'Organismo di Vigilanza mediante apposita delibera consiliare.

Al fine di garantire i requisiti di indipendenza e di autonomia, sono considerate cause di incompatibilità con l'incarico di componente dell'Organismo di Vigilanza dal momento della nomina e per tutta la durata della carica:

- essere componente esecutivo e/o non indipendente del Consiglio di amministrazione dell'Ente;
- avere relazioni di coniugio, parentela o affinità fino al quarto grado con i soggetti di cui ai punti precedenti;

- svolgere funzioni operative o di business all'interno dell'Ente, in qualità di dipendente;
- intrattenere significativi rapporti d'affari con l'Ente ed intrattenere significativi rapporti d'affari con i componenti del Consiglio di Amministrazione della stessa, che siano muniti, o meno, di deleghe;
- essere stati condannati, ovvero essere sottoposti ad indagine, per la commissione di uno dei Reati (nonché di reati o illeciti amministrativi di natura simile).

Al fine di garantire l'efficace e costante attuazione del Modello, nonché la continuità di azione, ed il mantenimento dei requisiti di indipendenza, la durata dell'incarico è fissata in un minimo di 12 mesi, fino ad un massimo di tre (3) anni, eventualmente rinnovabili con delibera del Consiglio di Amministrazione.

Rappresentano ipotesi di decadenza automatica le incompatibilità di cui sopra, la sopravvenuta incapacità e la morte; fatte salve le ipotesi di decadenza automatica, i componenti dell'Organismo possono essere revocati esclusivamente dal Consiglio di Amministrazione soltanto per giusta causa.

Rappresentano ipotesi di giusta causa di revoca:

- una sentenza di condanna dell'Ente ai sensi del Decreto o una sentenza di patteggiamento, passata in giudicato, ove risulti dagli atti l'"*omessa o insufficiente vigilanza*" da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- una sentenza di condanna o di patteggiamento emessa nei confronti di uno dei componenti dell'Organismo di Vigilanza per aver commesso uno dei Reati (o reati/illeciti amministrativi dello stesso genere);
- il mancato riserbo relativamente alle informazioni di cui vengano a conoscenza nell'espletamento dell'incarico;
- la mancata partecipazione a più di tre riunioni consecutive senza giustificato motivo
- un palese comportamento di omessa vigilanza.

Ciascun componente dell'OdV potrà recedere in ogni momento dall'incarico, mediante preavviso di almeno 1 (uno) mese, senza dover addurre alcuna motivazione.

In caso di dimissioni o di decadenza automatica di un componente effettivo dell'Organismo di Vigilanza, quest'ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione, che prenderà senza indugio le decisioni del caso.

L'Organismo di Vigilanza si intende decaduto se vengono a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, il Consiglio di Amministrazione provvede a nominare *ex novo* tutti i componenti.

6.2 FUNZIONI, POTERI ED ATTIVITA' DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza ha la funzione di vigilare costantemente:

- sull'osservanza del Modello da parte di tutti i Destinatari;
- sull'adeguatezza del Modello in relazione alla effettiva capacità di prevenire la commissione dei reati di cui al Decreto;
- sulla effettiva attuazione delle prescrizioni del Modello nell'ambito dello svolgimento delle attività dell'Ente;
- sull'aggiornamento del Modello, sull'attuazione e sull'effettiva funzionalità delle soluzioni ipotizzate (follow-up), proponendo al Consiglio di Amministrazione eventuali modifiche laddove si riscontrino esigenze di adeguamento al Modello, in

relazione ai mutamenti della struttura e dell'organizzazione societaria, del quadro normativo di riferimento o di altri eventi significativi.

In particolare, l'Organismo di Vigilanza ha i seguenti poteri:

- richiedere a tutti i destinatari del Modello informazioni e documentazione in merito alle operazioni ed agli atti compiuti nelle aree a rischio di commissione dei reati;
- adottare e/o attivare procedure di controllo al fine di verificare l'osservanza del presente Modello;
- effettuare verifiche a campione su determinate operazioni e/o atti specifici compiuti nelle aree a rischio di commissione dei reati;
- compiere indagini conoscitive al fine di individuare e/o aggiornare le "aree a rischio" di commissione dei reati;
- promuovere e/o sviluppare di concerto con l'Amministratore idonee iniziative per la diffusione, la conoscenza e la comprensione del presente Modello;
- fornire chiarimenti ed istruzioni per l'osservanza del presente Modello;
- consultarsi con l'Amministratore e/o consulenti esterni al fine di garantire l'efficacia del Modello;
- raccogliere, elaborare e custodire le informazioni relative al presente Modello;
- riferire periodicamente all'Amministratore Unico circa lo stato di attuazione e l'operatività del Modello;
- valutare e proporre all'Amministratore Unico le modifiche e/o gli aggiornamenti da apportare al presente Modello;
- disporre delle risorse opportune per lo sviluppo, monitoraggio e valutazione dell'efficacia del Modello.

L'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale.

L'Organismo dispone di autonomi poteri di spesa sulla base di un *budget* annuale approvato dal Consiglio di Amministrazione, su proposta dell'Organismo stesso, dando evidenza al Consiglio stesso delle spese effettuate.

L'Organismo può impegnare risorse che eccedono i propri poteri di spesa in presenza di situazioni eccezionali e urgenti, con l'obbligo di dare informazione al Consiglio di Amministrazione nella riunione immediatamente successiva.

L'Organismo di Vigilanza si dota sin dal primo insediamento di un Regolamento, ove sono specificati tutti gli aspetti rilevanti per il suo funzionamento, in particolare:

- gli ambiti di controllo e vigilanza.
- frequenza e modalità delle verifiche.
- frequenza e modalità di reporting.

6.3 REPORTING E SEGNALAZIONI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza redige periodiche relazioni sull'attività svolta, secondo le modalità e la frequenza stabilite nel proprio regolamento.

L'Organismo di Vigilanza comunica immediatamente al Consiglio di Amministrazione eventuali problematiche significative scaturite dall'attività di vigilanza effettuata e almeno annualmente relaziona per iscritto il Consiglio sull'attività svolta e sui risultati della stessa.

L'organismo di Vigilanza potrà ulteriormente essere invitato a relazionare periodicamente al Consiglio di Amministrazione in merito alle proprie attività.

L'Organismo di Vigilanza custodisce le relazioni ed i report generati dalle attività di sorveglianza e verifica effettuate.

6.4 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

In conformità a quanto disposto dal Decreto (art. 6, co. 2, lett. d), si stabilisce che:

- I Consiglieri sono tenuti a comunicare all'Organismo di Vigilanza ogni informazione utile allo svolgimento dell'attività di controllo e di verifica sull'osservanza del Modello, per assicurarne il funzionamento e la corretta attuazione;
- i medesimi obblighi informativi sono previsti in capo ai responsabili delle funzioni interessate dalle attività sensibili, che devono sempre riferire all'OdV eventuali anomalie nel seguire il Modello, nonché l'indicazione motivata dell'eventuale necessità di modifiche del Modello o dei suoi protocolli.
- i dipendenti e tutti i collaboratori esterni, sono tenuti a segnalare direttamente all'Organismo di Vigilanza le violazioni del Modello o delle procedure/protocolli stabiliti per la sua attuazione, nonché ogni altra informazione utile allo svolgimento dell'attività di controllo e alla verifica sull'adeguatezza del Modello.

E' vietata qualsiasi forma di ritorsione, discriminazione o penalizzazione nei confronti di coloro che effettuano in buona fede segnalazioni all'Organismo di Vigilanza. L'Ente si riserva ogni azione contro chiunque effettui in mala fede segnalazioni non veritiere.

L'Organismo di Vigilanza, nonché i soggetti dei quali l'Organismo, a qualsiasi titolo, si avvale, sono tenuti all'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni o attività.

In aggiunta alle segnalazioni di cui sopra, all'Organismo di Vigilanza devono essere obbligatoriamente ed immediatamente trasmesse, da chiunque ne abbia notizia:

- le richieste di assistenza legale inoltrate dai Dipendenti in caso di avvio di procedimento giudiziario per Reati compresi nel Modello;
- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini in ambito societario, eventualmente anche nei confronti di ignoti, per i Reati;
- l'evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate con specifico riferimento ai Reati ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

In particolare, i destinatari del Modello hanno l'obbligo di riportare ogni sospetta violazione del Modello all'Organismo di Vigilanza, inviando un'e-mail all'indirizzo del Presidente dell'OdV, che verrà reso noto.

L'Organismo agirà in modo da garantire i segnalanti in buona fede da qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando, altresì, la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti dell'Ente o delle persone coinvolte, nonché la reputazione del/dei segnalato/i.

L'Organismo di Vigilanza valuta con attenzione ed imparzialità le segnalazioni ricevute e può svolgere tutti gli accertamenti e gli approfondimenti all'uopo necessari.

7. INFORMAZIONE E FORMAZIONE

7.1 DIPENDENTI INTERNI

Ai fini dell'efficacia del presente Modello, è obiettivo dell'Ente garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti di tutti i dipendenti e di tutti i soggetti con funzione di gestione, amministrazione, direzione e controllo.

Tale obiettivo riguarda sia le risorse già presenti, sia quelle che ne faranno parte in futuro.

Il livello di formazione e comunicazione è attuato con un differente grado di approfondimento, in relazione al diverso livello di coinvolgimento delle risorse medesime nelle attività sensibili.

Il Consiglio di Amministrazione stabilisce il programma di formazione specifico per il presente Modello, e verifica personalmente che sia adeguato ed efficacemente attuato. Tale programma di formazione si inserisce nel più generale programma informativo e formativo rivolto al personale dell'Ente, che viene annualmente predisposto.

7.2 COLLABORATORI ESTERNI

I principi e i contenuti del Modello e del Codice Etico sono portati anche a conoscenza di tutti i soggetti che, pur non essendo lavoratori subordinati dell'Ente, operano per conto della stessa, svolgendo nel suo interesse prestazioni o servizi, quali collaboratori esterni, agenti, fornitori o altri soggetti che hanno rapporti contrattuali con l'Ente che implicano lo svolgimento di attività in favore o per conto del medesimo.

L'impegno al rispetto della legge e dei principi di riferimento del Modello da parte di tali soggetti dovrà essere previsto da apposita clausola del relativo contratto.

Tale clausola dovrà inoltre prevedere la facoltà per l'Ente di procedere all'applicazione di forme di autotutela (ad esempio risoluzione del contratto, applicazione di penali etc.) laddove sia ravvisata una violazione dei principi e dei contenuti del Modello.

8. SISTEMA SANZIONATORIO

8.1 PRINCIPI GENERALI

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

Il rispetto delle disposizione del Modello vale ed è vincolante nell'ambito dei rapporti di lavoro o di incarico di qualsiasi tipologia e natura, inclusi quelli con Amministratori, dirigenti, collaboratori a progetto, part-time, nonché negli altri contratti di collaborazione. L'applicazione di sanzioni disciplinari per violazione delle regole di condotta prescinde dall'esito del giudizio penale, in quanto tali regole sono assunte dalla Società in piena autonomia e a prescindere dall'illecito che eventuali condotte possano determinare.

Le sanzioni applicabili in caso di violazione delle regole e delle procedure previste dall'Ente sono state dettagliatamente descritte nell'allegato B denominato "Sistema disciplinare e sanzionatorio" che è stato espressamente approvato con delibera del Consiglio di Amministrazione, unitamente al presente Modello, e a cui ci si richiama integralmente.

**PARTE SPECIALE A
I REATI CONTRO LA PUBBLICA
AMMINISTRAZIONE ED I REATI CONTRO
L'AMMINISTRAZIONE DELLA GIUSTIZIA**

9. PARTE SPECIALE A - I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE ED I REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA

9.1 FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la Pubblica Amministrazione e a quelli realizzabili nelle relazioni e nei contatti con l'Autorità Giudiziaria.

I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

I reati contro la Pubblica Amministrazione sono disciplinati dal Titolo II, del Libro secondo, del Codice Penale.

Tra le fattispecie penali qui considerate alcune determinano nocimento alla "Pubblica Amministrazione", che è da intendersi quale aggregazione di tutti gli Enti che "svolgono tutte le attività dello Stato e degli altri Enti pubblici" inclusi, quindi, anche gli Stati esteri, gli Organi Comunitari e le emanazioni estere dello Stato.

Agli effetti della legge penale, si considera Pubblica Amministrazione qualsiasi persona giuridica che persegua e/o realizzi e gestisca interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, disciplinata da norme di diritto pubblico e manifestantesi mediante atti autoritativi.

A titolo meramente esemplificativo ed avendo riguardo all'operatività dell'Ente si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione: (i) lo Stato, le Regioni, le Province, i Comuni; ii) i Ministeri, i Dipartimenti, le Commissioni; (iii) gli Enti Pubblici non economici (INPS, INAIL, ISTAT); (iv) altri Enti Pubblici (ASL, Guardia di Finanza, Agenzia delle Entrate, ecc.).

Altre fattispecie penali qui considerate presuppongono, invece, il coinvolgimento di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" e/o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p..

Nella realtà, la distinzione tra le due figure è basata sulla funzione oggettivamente svolta dai soggetti in questione:

- la qualifica di Pubblico Ufficiale è attribuita a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. A titolo meramente esemplificativo si possono menzionare i seguenti soggetti, nei quali la giurisprudenza ha individuato la qualifica di Pubblico Ufficiale: ufficiale giudiziario, consulente tecnico del giudice, esattore di aziende municipalizzate, portalettere;
- la qualifica di Incaricato di Pubblico Servizio si determina per via di esclusione, spettando a coloro che svolgono quelle attività di interesse pubblico, non consistenti in semplici mansioni d'ordine o meramente materiali, disciplinate nelle stesse forme della pubblica funzione, ma alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale. A titolo esemplificativo si elencano i seguenti soggetti nei quali la giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, lettori dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza.

Va considerato che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un Ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato.

In relazione al soggetto passivo del reato, sono parificati ai Pubblici Ufficiali e agli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana quei

soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità europee, o nell'ambito di Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale.

Si indicano brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 agli artt. 24, 25 e 25-*decies*, rimandandosi al testo del decreto e a quello del Codice Penale per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Cod. Pen.

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

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti, sovvenzioni o contributi dallo Stato italiano, altro ente pubblico o dalle Comunità Europee, destinati a favorire iniziative dirette alla realizzazione di opere oppure allo svolgimento di attività di pubblico interesse, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

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

Il rischio che il presente reato possa essere commesso nell'attività dell'Ente deriva dai casi in cui l'Ente richiede ed utilizza finanziamenti pubblici (erogati direttamente o per il tramite di società terza capofila), sia a livello di organi direzionali che a livello operativo (Amministrazione e Controllo, Area Formazione).

Il reato può configurarsi, ad esempio, utilizzando i fondi ricevuti per l'acquisto o la realizzazione di attività diverse rispetto a quelle di destinazione, manipolando i dati di rendicontazione al fine di far figurare spese in realtà sostenute per altri scopi, ecc.

▪ **Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316 ter c.p.)**

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

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

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

Il rischio della configurazione di detto reato nell'attività sociale può esserci quando si richiedono finanziamenti pubblici (direttamente o per il tramite di società terza capofila) sia a livello di organi direzionali che a livello operativo (Amministrazione e Controllo, Area Formazione). Ipotesi tipica è presentare documenti falsi o manipolati per attestare l'esistenza di condizioni di partecipazione ad una gara.

▪ **Concussione (art. 317 c.p.)**

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale (è, quindi, reato c.d. proprio), abusando della sua posizione, costringa taluno a dare o a promettere a sé o ad altri, denaro o altre utilità non dovutegli.

Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.Lgs. 231/2001; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del D.Lgs. 231/2001 stesso, nell'ipotesi in cui un dipendente od un agente dell'azienda concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per l'Ente).

▪ **Corruzione per l'esercizio della funzione (art. 318 c.p.)**

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceva, per sé o per un terzo, denaro o altra utilità o ne accetti la promessa. Ai sensi dell'art. 320 c.p., è punito anche l'incaricato di pubblico servizio che tenga la condotta prima descritta.

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

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per omettere o ritardare 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, riceva, per sé o per un terzo, denaro od altra utilità, o ne accetti la promessa. Ai sensi dell'art. 320 c.p., è punito anche l'incaricato di pubblico servizio che tenga la condotta prima descritta.

Le ipotesi di cui agli art. 318 e 319 c.p. si differenziano dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

▪ **Corruzione in atti giudiziari (art. 319 ter c.p.)**

Tale ipotesi di reato si configura nel caso i fatti indicati negli articoli 318 e 319 siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

▪ **Pene per il corruttore e istigazione alla corruzione (artt. 321 e 322 c.p.)**

E' punito chiunque ponga in essere un comportamento finalizzato alla corruzione (es. offre o promette denaro ad un pubblico ufficiale), sia ove il pubblico ufficiale o l'incaricato di un pubblico servizio accetti l'offerta o la promessa (art. 321 c.p.) sia ove le rifiuti (art. 322 c.p.).

▪ **Induzione indebita a dare o promettere utilità (art. 319 quater c.p., inserito dall'art. 1, comma 75, l. 6 novembre 2012, n. 190)**

Ove il pubblico ufficiale o l'incaricato di pubblico servizio, 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, viene punito, oltre al Pubblico ufficiale o all'incaricato di pubblico servizio, anche il soggetto indotto.

▪ **Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.)**

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato o di altro Ente Pubblico.

Tale reato può realizzarsi, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni da parte dello Stato, di altri enti pubblici o delle Comunità europee.

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

▪ **Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter c.p.)**

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando un danno allo Stato o ad altro ente pubblico. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente. Un altro esempio di commissione del reato è l'alterazione

dei dati del software di gestione della rendicontazione contributi DOCUP o la modifica dati previdenziali o fiscali già comunicati alla P.A., anche per il tramite dei consulenti esterni (commercialista, consulente del lavoro, ecc.).

I REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA

I reati contro l'Amministrazione della Giustizia, ossia l'induzione a non rendere dichiarazioni all'Autorità giudiziaria e l'induzione a rendere dichiarazioni mendaci all'Autorità giudiziaria, sono previsti e puniti dall'art. 377-bis c.p.

Si indicano, brevemente, qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 all'art. 25-decies, rimandandosi al testo del decreto e a quello del Codice Penale per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Cod. Pen.

- **Induzione a non rendere dichiarazioni all'Autorità giudiziaria (art. 377 bis, prima parte, c.p.)**

Tale ipotesi di reato doloso si configura nel caso in cui, mediante violenza (coazione fisica o morale) minaccia, offerta o promessa di denaro o di altra utilità, si induce taluno a non rendere dichiarazioni all'Autorità giudiziaria, ove queste siano utilizzabili in un procedimento penale.

- **Induzione a rendere dichiarazioni mendaci all'Autorità giudiziaria (art. 377 bis, seconda parte, c.p.)**

Tale ipotesi di reato doloso si configura nei casi in cui, mediante violenza (coazione fisica o morale) minaccia, offerta o promessa di denaro o di altra utilità, si induce taluno a rendere dichiarazioni mendaci all'Autorità giudiziaria, ove queste siano utilizzabili in un procedimento penale.

9.1.1 Esclusioni

Non si rilevano esclusioni fra i reati di cui alla presente parte speciale.

9.1.2 Individuazione dei processi sensibili

I principali Processi Sensibili, che l'Ente ha individuato al proprio interno sono i seguenti:

- richieste di finanziamenti e contributi pubblici (in particolare per le attività formative e di aggiornamento, di affiancamento e consulenza per la ricerca del lavoro, che sono oggetto della specifica attività aziendale)
- rapporti correnti con la Pubblica Amministrazione;
- rapporti con l'Autorità Giudiziaria;
- gestione delle ispezioni esterne (amministrative, fiscali, previdenziali, ecc.);
- acquisti di beni e servizi;
- gestione delle risorse finanziarie;
- gestione del Personale;
- gestione del servizio di formazione – rapporto con i fornitori
- gestione di regali e omaggi
- utilizzo della firma digitale e della rete internet

9.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione.

Sono, quindi, definite a rischio tutte le aree che per lo svolgimento della propria attività intrattengono rapporti con la Pubblica Amministrazione o gestiscono risorse finanziarie

che potrebbero essere impiegate per attribuire vantaggi ed utilità a pubblici ufficiali (c.d. "rischio indiretto").

In particolare, in seguito all'attività di risk assessment, effettuata dall'Ente, sono state individuate nella gestione dei rapporti con enti pubblici (Regione, Provincia, Comuni, ASL, Guardia di Finanza, Agenzia delle Entrate, ecc.) le seguenti attività considerate a rischio.

9.2.1 Richiesta finanziamenti e contributi pubblici

Il processo riguarda quelle attività volte ad acquisire e gestire i contributi, le sovvenzioni ed i finanziamenti concessi da soggetti pubblici, in particolare la Regione Veneto (attività di formazione e di ricerca del lavoro).

Il processo si articola nelle seguenti fasi:

- individuazione del bando regionale e dei soggetti interessati;
- elaborazione del progetto da parte di TerServizi, compilazione ed invio della domanda, in qualità di Ente attuatore;
- attuazione del piano e rendicontazione dei costi di progetto;
- gestione delle verifiche ed ispezioni da parte dell'Ente finanziatore;
- pagamento delle fatture dei docenti e fornitori in genere.

In relazione a questo processo, i reati ipotizzabili potrebbero essere la concussione, la corruzione, l'induzione indebita a dare o promettere utilità, l'indebita percezione di erogazioni, la malversazione e in via subordinata la truffa a danno dello Stato.

I reati di concussione o di corruzione potrebbero essere commessi per rendere più facile l'assegnazione del finanziamento a favore dell'Ente

Il reato di indebita percezione di erogazioni potrebbe essere commesso al momento della richiesta dello stanziamento del finanziamento concesso e dell'acquisizione del finanziamento mediante la presentazione di richieste di finanziamento che contengano dichiarazioni o documenti falsi che attestino dati o fatti non veri o omettano informazioni dovute.

Il reato di malversazione potrebbe essere commesso nel caso in cui i fondi ottenuti vengano destinati a scopi diversi da quelli dichiarati.

Il reato di truffa a danno dello Stato potrebbe essere addebitato, in caso non sia possibile procedere per i reati precedentemente descritti, nelle fasi di presentazione della domanda di finanziamento, di attuazione del progetto, di collaudo e di eventuali controlli, a mero titolo esemplificativo e non esaustivo, attraverso la predisposizione e diffusione di documenti non veritieri, con conseguente danno patrimoniale per lo Stato.

Il sistema di controllo si basa sulla registrazione di ogni attività all'interno del CRM, con tracciabilità dell'intero processo, sulla gestione rigorosa dei flussi relativi a finanziamenti/contributi in entrata e in uscita; sulla registrazione dei vari atti e sulla effettuazione di specifiche attività di sorveglianza e verifica.

Il protocollo che si è dato l'Ente è il seguente:

- Individuazione del bando/progetto effettuata da parte del personale o dei collaboratori esterni di Ter Servizi;
- Decisione di presentare uno o più progetti assunta dal coordinatore del personale sulla base delle indicazioni fornite annualmente dal Consiglio di Amministrazione;
- Apertura del progetto all'interno del CRM aziendale, con obbligo di registrare ogni attività relativa allo stesso;
- Incarico formalizzato al collaboratore esterno per la redazione del progetto unitamente al soggetto interno che se ne occupa;

- Scelta del docente tramite il proprio data base – che contiene anche la valutazione su ciascun fornitore- e conferimento dell’incarico con apposita lettera scritta con clausola risolutiva espressa in caso di violazione della normativa 231.
- Sottoscrizione dell’apposito regolamento da parte del Docente.
- Monitoraggio/controllo dell’attività dei docenti.
- Archiviazione e conservazione di tutta la documentazione inerente, ivi inclusa quella trasmessa anche in via telematica o elettronica.
- Autocertificazione richiesta su tutti i dati che provengono da terzi.
- Controlli interni durante la tenuta dei corsi/seminari da parte di un dipendente;
- Gestione finanziaria in accordo con le regole poste dai Bandi e dagli Enti erogatori
- La verifica della rendicontazione, al termine del progetto, viene effettuata da parte di Ispettori esterni di volta in volta incaricati dagli Enti erogatori, e comunque sempre dal Revisore ed assistiti dal responsabile amministrativo.
- Informazione all’OdV sia della richiesta che dell’ottenimento del finanziamento, nonché dell’atto conclusivo dello stesso.

9.2.2 Gestione rapporti con gli enti pubblici per rilascio autorizzazioni e/o obblighi di informativa

Le comunicazioni all’Agenzia delle Entrate, all’Inps e all’Inail e altri uffici pubblici vengono curate dal personale addetto e con l’eventuale ausilio di consulenti esterni appositamente incaricati per iscritto.

Per quanto attiene eventuali rapporti con il Comune ed altri enti della P.A., qualsiasi comunicazione/ richiesta è tracciata attraverso mezzi telematici.

In relazione a questi ambiti di attività, i reati ipotizzabili, in linea di principio, potrebbero essere la concussione, la corruzione e la truffa a danno dello Stato.

I reati di corruzione o induzione indebita a dare o promettere utilità potrebbero essere consumati attraverso il contatto con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore (o a minor sfavore) per l’Ente.

Il reato di truffa a danno dello Stato potrebbe configurarsi in una rappresentazione non trasparente dei fatti, tramite l’emissione di documenti o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno allo Stato.

Il processo di gestione dei rapporti con la Pubblica Amministrazione in occasione di richieste di autorizzazioni e concessioni, trasmissione di informative ecc. si articola nelle seguenti fasi:

- predisposizione della documentazione;
- raccolta della firma del Presidente del CdA;
- invio della documentazione e archiviazione della pratica;
- gestione dei rapporti con gli Enti pubblici.

Il sistema di controllo si basa sulla tracciabilità dei vari atti, sulla segregazione delle funzioni, sull’effettuazione di specifiche attività di riscontro.

Il protocollo che si è dato l’Ente è il seguente:

Le attività devono essere svolte in modo tale da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell’istanza di autorizzazione/comunicazione, o forniti in esecuzione degli adempimenti, prevedendo, ove opportuno, gli specifici controlli.

In particolare:

- laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della predisposizione dei documenti richiesti dall'Ente pubblico, è effettuato un controllo sulla correttezza delle elaborazioni da parte del responsabile della funzione coinvolta nel procedimento;
- gli eventuali rapporti con l'Ente pubblico interessato sono curati, oltre che dal personale interno incaricato, dall'Amministratore Delegato; in caso di richieste non eseguite per via telematica, è autorizzato a recarsi presso l'Ente pubblico unicamente il Presidente del CdA o l'Amministratore Delegato;
- la tracciabilità del processo è garantita tramite l'archiviazione di copia della documentazione consegnata o trasmessa, anche in via telematica o elettronica, all'Ente pubblico;

Nel caso di incarico assegnato a consulenti di operare in rappresentanza o nell'interesse dell'Ente nei confronti della Pubblica Amministrazione deve essere prevista la forma scritta e deve essere inserita una specifica clausola contrattuale di adesione al "Modello 231" vigente in Ter Servizi.

Costituisce in questo caso un presidio specifico il controllo che l'OdV potrà fare in tutte le fasi del processo.

9.2.3 Verifiche e ispezioni svolte da soggetti esterni

Il processo riguarda l'attività di verifiche ed ispezioni svolte da parte della Pubblica Amministrazione (es. Guardia di Finanza, ASL, NAS, ecc.).

Il processo di gestione dei rapporti con la Pubblica Amministrazione in occasione di verifiche e ispezioni si articola nelle seguenti fasi:

- gestione dei rapporti con i rappresentanti della Pubblica Amministrazione;
- eventuale predisposizione e consegna della documentazione richiesta;
- eventuale firma del verbale di fine ispezione.

In relazione a questo processo, i reati ipotizzabili, in linea di principio, potrebbero essere la concussione, la corruzione e la truffa a danno dello Stato.

I reati di concussione, corruzione o induzione indebita a dare o promettere utilità, potrebbero essere commessi tramite la presenza del contatto con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore (o a minor sfavore) per l'Ente.

Il reato di truffa a danno dello Stato potrebbe configurarsi in una rappresentazione non trasparente della realtà, tramite l'emissione di documenti, o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno allo Stato.

Gli elementi specifici di controllo e presidio si basano su livelli autorizzativi definiti, sulla segregazione delle funzioni, sulla tracciabilità e sulla valutazione complessiva dell'attività, nonché su una precisa procedura denominata "PROCEDURA INTERNA PER LA GESTIONE DEL RICEVIMENTO VISITE ISPETTIVE".

La tracciabilità del processo è garantita tramite la registrazione e l'archiviazione degli atti e dei documenti (es. verbale di ispezione, copie della documentazione fornita, ecc.) inerenti ogni specifica verifica o ispezione.

L'Ente richiede a tutti i soggetti che hanno assistito a visite ed ispezioni da parte della Pubblica Amministrazione, di rendicontare tempestivamente in merito; in particolare

viene individuato un soggetto che deve trasmettere l'esito della verifica al Consiglio di Amministrazione

9.2.4 Rapporti con l'Autorità Giudiziaria

Al fine di evitare le condotte di cui all'art. 377 bis c.p., l'Ente, oltre ai precedenti presidi specifici nei rapporti con la Pubblica Amministrazione, ha approvato il Codice Etico cui si devono attenere tutti i soggetti agenti all'interno di Ter Servizi e i collaboratori esterni.

Nel caso di procedimento penale civile o amministrativo che possa coinvolgere il personale a qualsiasi livello di Ter Servizi, chiunque ne abbia notizia è tenuto ad informare l'OdV e il Consiglio di Amministrazione, che curerà l'aggiornamento all'OdV dell'iter processuale.

Nel corso dei processi penali, civili o amministrativi, è fatto divieto di intraprendere alcuna azione illecita che possa favorire l'Ente. E' fatto poi divieto di intraprendere alcuna azione illecita che possa favorire o danneggiare una delle parti del processo anche qualora l'Ente non sia parte in causa.

9.2.5 Acquisti di beni e servizi

Il processo di acquisizione di beni (es. materiale d'uso comune, ecc.), di manutenzioni (elettricista, idraulico, manutenzioni varie, ecc.) e di servizi per la formazione (Es. docenza per i corsi di formazione, consulenze esterne, tutoraggio esterno, pulizia-ecc.,) si può generalizzare nelle seguenti fasi:

- Richiesta della fornitura;
- Autorizzazione della fornitura;
- Scelta del fornitore e stipulazione del contratto oppure trasmissione dell'offerta sottoscritta;
- Gestione operativa del contratto/ordine (consegna beni / esecuzione prestazioni);
- contabilizzazione e pagamento fatture.

Il processo di acquisizione di beni e servizi costituisce una delle modalità strumentali attraverso cui, in linea di principio, possono essere commessi i reati di concussione, corruzione, anche tra privati (come si vedrà nella Parte Speciale relativa ai Reati Societari), o di induzione indebita a dare o promettere utilità, nonché, come si dirà nella Parte Speciale C, i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

I reati di corruzione o di induzione indebita a dare o promettere utilità, potrebbero essere consumati attraverso la gestione non trasparente del processo di acquisizione (ad es. con l'assegnazione di contratti o di ordini di acquisto a persone o società "gradite" ai soggetti della Pubblica Amministrazione, per ottenere in cambio favori nell'ambito dello svolgimento di altre attività aziendali).

Il sistema di controllo si basa sulla separazione di ruolo nelle fasi chiave del processo, sulla registrazione dei vari atti e sulla comunicazione di eventuali anomalie all'OdV.

I Principi generali da osservare in tutti i processi di acquisto di beni che di servizi d'importo superiore ad euro 500,00 e non relativi ai servizi alla formazione ~~o di beni che di servizi~~, sono:

1. Esistenza di soggetti diversi operanti nelle seguenti fasi/attività del processo:
 - individuazione di almeno 3 fornitori del bene/servizio;
 - autorizzazione della fornitura da parte dell'Amministratore Delegato;
 - autorizzazione per i pagamenti da parte dell'Amministratore Delegato
 - effettuazione dell'acquisto da parte di soggetto delegato;

2. Esistenza di criteri tecnico-economici per la selezione di potenziali fornitori:
 - Espletamento di adeguata attività selettiva fra diversi offerenti, e di obbiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili o di espressa procedura).
 - Esistenza di un data base per la scelta dei docenti.
 - Utilizzo di dispositivi contrattuali adeguatamente formalizzati.
3. Registrazione e archiviazione delle singole fasi del processo (documentazione a supporto, formalizzazione e modalità/tempistiche di archiviazione), in modo tale che sia possibile la ricostruzione delle responsabilità, delle motivazioni, delle scelte e delle fonti informative.

Referente è l'Ufficio Amministrativo.

L'ordine è confrontato con la fattura da parte del Responsabile Amministrativo.

9.2.6 Gestione regali e omaggi

Il processo è caratterizzato da tutte quelle attività relative alla distribuzione gratuita di beni e servizi, a clienti, fornitori, rete commerciale, ecc. con l'obiettivo primario di sviluppare l'attività commerciale, promuovendo la domanda dei servizi erogati dall'Ente.

Non è consentito corrispondere né offrire, direttamente o indirettamente, pagamenti e benefici materiali di qualsiasi entità a terzi, pubblici ufficiali o privati, per influenzare o compensare un atto del loro ufficio o una condotta di favore.

Gli atti di cortesia commerciale, come regali, omaggi o forme di ospitalità, sono consentiti quando siano di modico valore e tali da non compromettere l'integrità o la reputazione di una delle parti e da non poter essere interpretati, da un osservatore imparziale, come finalizzati ad acquisire vantaggi in modo improprio.

Ai dipendenti è fatto divieto di accettare omaggi o trattamenti di favore non direttamente ascrivibili a normali relazioni di cortesia. Ai collaboratori esterni viene formalmente richiesto di attenersi ai principi contenuti nel Codice Etico, con l'esplicita previsione di risoluzione di diritto dal rapporto in caso di inadempimento.

Il processo degli omaggi, che viene gestito con le stesse modalità degli acquisti di cui sopra, è una delle modalità strumentali attraverso la quale, in linea di principio, può essere commesso il reato di concussione, corruzione, anche tra privati (come si specificherà nella Parte Speciale relativa ai Reati Societari), e di induzione indebita a dare o promettere utilità, oltre che i reati di ricettazione, riciclaggio e autoriciclaggio.

La gestione anomala di questo processo potrebbe costituire un potenziale supporto alla commissione del reato verso dipendenti pubblici ed amministratori per ottenere trattamenti di favore nell'ambito dello svolgimento di altre attività sociali.

Oltre al presidio generale previsto dal Codice Etico, sussistono in ogni caso presidi specifici:

- tutte le uscite di denaro sono tracciate e documentate e l'utilizzo del contante è limitato al minimo;
- gli eventuali omaggi non possono superare il costo unitario di € 50,00;
- registro degli omaggi con indicazione del destinatario e della data di consegna.

9.2.7 Gestione del personale

Il processo di selezione, assunzione e gestione del personale è formato da tutte le attività necessarie alla costituzione del rapporto di lavoro tra l'Ente e una persona fisica e alla successiva gestione. Vigeva una consolidata prassi che coinvolge le modalità di assunzione del personale, formazione del personale, attribuzione di *bonus* o aumenti ed irrogazione di provvedimenti disciplinari.

In Ter Servizi trova applicazione il CCNL Commercio, inoltre, l'Ente si è dotata di apposito Regolamento per il personale, sottoscritto da ciascun dipendente al momento dell'assunzione.

Il personale dipendente è stabile da anni e eventuali esigenze di nuove assunzioni vengono portate all'attenzione del Consiglio di Amministrazione.

Il Potere Disciplinare viene esercitato dal Consiglio di Amministrazione, tranne che nel caso di violazioni delle norme sulla sicurezza e salute negli ambienti di lavoro, per le quali si fa riferimento al nominato D.L.

In tutti i casi il procedimento viene svolto nel pieno rispetto delle previsioni contenute nel CCNL applicato, secondo apposito *iter*:

- Contestazione disciplinare scritta a firma dell'Datore di lavoro;
- Controdeduzioni da parte del dipendente;
- Eventuale erogazione del provvedimento disciplinare.

La procedura risulta completamente tracciata.

Il processo in oggetto potrebbe costituire una delle modalità strumentali attraverso cui commettere il reato di concussione, corruzione o induzione indebita a dare o promettere utilità.

Una condotta non trasparente nelle varie fasi di gestione del personale, potrebbe consentire la commissione di tale reato attraverso, ad esempio, la promessa di assunzione verso rappresentanti della Pubblica Amministrazione, o soggetti da questi indicati, al fine di ottenerne favori o vantaggi nell'ambito dello svolgimento di altre attività sociali.

9.2.8 Principi generali di comportamento e di attuazione dei processi nelle aree di attività a rischio

Nelle relazioni con gli esponenti della Pubblica Amministrazione con cui l'Ente intrattiene rapporti (dirigenti, funzionari, dipendenti della Pubblica Amministrazione, suoi consulenti o collaboratori esterni od incaricati *ad acta*), con interlocutori commerciali privati in rappresentanza di enti concessionari di pubblico servizio, nonché, più in generale, con tutti gli interlocutori, anche privati, di Ter Servizi, è fatto divieto di:

- promettere od offrire loro denaro od omaggi salvo che si tratti di omaggi o utilità d'uso di modico valore e comunque nel rispetto del presente Modello;
- qualsiasi forma di regalo a dipendenti della Pubblica Amministrazione o a loro familiari che possa influenzarne l'imparzialità ovvero l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;
- esaminare o proporre a dipendenti, consulenti o collaboratori della Pubblica Amministrazione opportunità commerciali o utilità di qualsiasi altro genere, per sé stessi od altri, che possano avvantaggiarli in modo indebito;
- promettere od offrire, a loro od a terze persone da costoro segnalate, la prestazione di consulenze di qualunque genere e a qualunque titolo;
- promettere o fornire loro, od a terze persone da costoro segnalate, servizi o lavori di utilità personale;

- favorire, nei processi d'acquisto, fornitori e sub-fornitori in quanto indicati dai dipendenti, da consulenti o collaboratori della Pubblica Amministrazione come condizione per lo svolgimento successivo delle attività. Tali azioni sono vietate tanto se poste in essere direttamente dall'Ente tramite i propri dipendenti, tanto se realizzati indirettamente tramite persone non dipendenti che agiscano per conto dell'Ente stesso;
- di offrire o di accettare qualsiasi oggetto, servizio, prestazione o favore di valore per ottenere un trattamento più favorevole in relazione a qualsiasi rapporto intrattenuto con la Pubblica Amministrazione.

Nei confronti della Pubblica Amministrazione è fatto inoltre divieto di:

- predisporre od esibire documenti falsi o alterati;
- sottrarre od omettere di presentare documenti veritieri;
- tenere una condotta ingannevole, che possa indurre la Pubblica Amministrazione in errore nella valutazione tecnico-economica dei servizi offerti;
- omettere informazioni dovute, al fine di orientare indebitamente le decisioni della Pubblica Amministrazione o, comunque, fornire informazioni non veritiere o tendenziose;
- farsi rappresentare da consulenti o da soggetti terzi quando tale situazione possa creare conflitti d'interesse;

Le relazioni con i fornitori sono regolate dai principi, dalle procedure e dalle regole previsti nel Modello 231 e sono oggetto di un costante monitoraggio.

Tali relazioni comprendono i contratti di consulenza e di docenza.

La stipula di un contratto con un fornitore deve sempre basarsi su rapporti di estrema chiarezza.

Per garantire la massima trasparenza ed efficienza del processo di acquisto, l'Ente predispone la conservazione delle informazioni nonché dei documenti ufficiali e contrattuali per i periodi stabiliti dalle normative vigenti e secondo le modalità previste nel presente Modello.

9.3 FLUSSI INFORMATIVI VERSO L'ODV

I flussi sono regolati secondo quanto previsto al paragrafo 6.4 della parte Generale del presente modello.

PARTE SPECIALE B

I DELITTI INFORMATICI ED I REATI CON VIOLAZIONE DEI DIRITTI D'AUTORE

10. PARTE SPECIALE B - I DELITTI INFORMATICI ED I REATI CON VIOLAZIONE DEI DIRITTI D'AUTORE

10.1 FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati di accesso abuso o alterazione di sistemi informatici o telematici, di danneggiamento o di frode e falsità in relazione a documenti e programmi informatici, nonché ai reati commessi con violazione dei diritti d'autore. Si indicano brevemente qui di seguito, dopo le Definizioni, le singole fattispecie contemplate nel D.Lgs. 231/2001 agli artt. 24 bis e 25 novies, rimandandosi al testo del decreto, al Codice Penale ed a quello della legge 633 del 1941 e ss. mm. E ii. (L.A.) per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Codice Penale.

Definizioni

- *Credenziali*: l'insieme degli elementi identificativi di un utente o di un account (generalmente UserID e Password).
- *Dati Informatici*: qualunque rappresentazione di fatti, informazioni, o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.
- *Delitti in Violazione del Diritto d'Autore*: i reati di cui all'art. 25 novies del Decreto.
- *Delitti Informatici*: i reati di cui all'art. 24bis del Decreto.
- *Utente*: ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione.
- *Documento/i Informatico/i*: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- *Firma Elettronica*: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
- *L.A. o Legge sul Diritto d'Autore*: Legge 22 aprile 1941 n. 633 sul diritto d'autore.
- *Password*: sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.
- *Peer to Peer*: meccanismo di condivisione di contenuti digitali tramite una rete di personal computer, di regola utilizzati per scambio di file con contenuti audio, video, dati e software.
- *Postazione di Lavoro*: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.
- *Sicurezza Informatica*: l'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.
- *Sistema Informatico*: complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, bit, in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.
- *Spamming*: invio di numerosi messaggi indesiderati, di regola attuato attraverso l'utilizzo della posta elettronica. *Virus*: programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di

distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.

DELITTI INFORMATICI

▪ **Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)**

Questo articolo stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. Capo III, Titolo VII, Libro II), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un Documento Informatico, pubblico o privato, avente efficacia probatoria (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).

Le 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.

A titolo esemplificativo, integra il delitto di falsità in Documenti Informatici la condotta di chi falsifichi documenti aziendali oggetto di flussi informatizzati ovvero la formazione di un documento informatico attestante dati falsi e firmato digitalmente, avente quindi efficacia probatoria, nonché la condotta di chi alteri informazioni a valenza probatoria presenti sui sistemi aziendali allo scopo di eliminare dati ritenuti rilevanti in vista di una possibile attività ispettiva.

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

Tale ipotesi di reato si configura nei casi in cui un soggetto, abusivamente, si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La tutela è rivolta alla salvaguardia del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto.

Il delitto si perfeziona con la violazione del domicilio informatico, anche la semplice visualizzazione, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario il danneggiamento del sistema altrui.

La fattispecie potrebbe realizzarsi nell'ipotesi in cui un soggetto operante nell'interesse dell'Ente, acceda abusivamente ai sistemi informatici di proprietà di terzi (es. un concorrente), per acquisire informazioni sull'operato altrui nell'ambito di una negoziazione commerciale, es. visione delle offerte di un concorrente.

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

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto 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 fornisca indicazioni o istruzioni idonee al predetto scopo.

Questo articolo punisce le condotte preliminari all'accesso abusivo, consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso (es. Password o smart card), necessari per superare le barriere protettive di un sistema informatico. Potrebbe rispondere del delitto, ad esempio, il dipendente dell'Ente che comunichi ad un altro soggetto, ad es. un amministratore, la Password di accesso alla e-mail di un proprio collega, allo scopo di garantire all'amministratore la possibilità di controllare le attività svolte dallo stesso, quando da ciò possa derivare un determinato vantaggio o interesse per l'Ente.

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

Tale ipotesi di reato punisce chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Tale delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un virus che poi immetta nel sistema informatico dell'Ente concorrente in modo da interromperne il funzionamento.

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

Tale ipotesi di reato si configura nel caso in cui un soggetto fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa.

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 suddette comunicazioni.

Questo reato è configurabile a carico del dipendente/amministratore, che per far ottenere un vantaggio all'Ente, interrompa il flusso delle comunicazioni telematiche di uno o più concorrenti.

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

Punisce chi, 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.

L'Ente potrebbe rispondere per questo reato presupposto nell'ipotesi un dipendente installasse un'apparecchiatura per intercettare le comunicazioni informatiche nel sistema di un concorrente.

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

Punisce chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Sarebbe configurabile un vantaggio in capo all'Ente ove tale danneggiamento fosse compiuto da un soggetto operante per conto della stessa per far venire meno la prova del credito da parte di un fornitore dell'Ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo.

- **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.)**

Punisce chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Tale reato può, ad esempio, essere commesso nell'interesse dell'Ente qualora un dipendente alteri documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. Procura) relativi ad un procedimento penale a carico dell'Ente.

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

Punisce chi, mediante 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.

Pertanto qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di

danneggiamento dei sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p.

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

Punisce chi distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Sono puniti anche la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

▪ **Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)**

Punisce 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.

DELITTI CON VIOLAZIONE DEI DIRITTI D'AUTORE

▪ **Protezione dell'opera di ingegno (art. 171 comma 1, lett. a bis L.A.)**

Tale reato si configura quando si mette a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, un'opera di ingegno protetta o parte di essa.

Ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.

L'Ente potrebbe rispondere di tale reato nel caso venissero caricati nel sito internet della stessa dei contenuti coperti dal diritto d'autore.

▪ **Protezione dell'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima (art. 171 comma 3 L.A.)**

Tale reato si configura nella messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Il bene giuridico qui protetto è l'onore e la reputazione del titolare dell'opera.

L'Ente potrebbe rispondere di tale reato nel caso venissero caricati nel sito internet della stessa dei contenuti coperti dal diritto d'autore, ma modificati in tal modo da ledere la reputazione dell'autore dell'opera.

▪ **Protezione del software e delle banche dati (art. 171 bis L.A.)**

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

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

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

Lo stesso fatto è punito anche se la condotta abbia ad oggetto un qualsiasi mezzo inteso a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratore.

Il secondo comma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue

l'estrazione o il reimpiego della banca di dati ovvero distribuisce, vende o concede in locazione una banca di dati.

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

Tale reato potrebbe ad esempio essere commesso nell'interesse dell'Ente qualora venissero utilizzati, per scopi lavorativi, programmi non originali al fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un software originale.

Sono rilevanti le attività aziendali in cui si ricorre all'uso di programmi o software informatici. In questo ambito possono rientrare anche comportamenti volti a riprodurre su supporti non contrassegnati SIAE o a distribuire il contenuto di una banca di dati in violazione delle disposizioni normative previste per l'accesso a banche dati.

▪ **Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico di opere dell'ingegno (art.171-ter L.A.)**

Tale ipotesi di reato si configura nel caso in cui, a fini di lucro, per uso non personale:

- a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
- b) abusivamente riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati;
- c) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuzione, mette in commercio, concede in noleggio o cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo televisione con qualsiasi procedimento, trasmette a mezzo radio, duplicazioni o riproduzioni abusive di cui alle lettere a) e b) senza aver concorso nella duplicazione o riproduzione;
- d) detiene per la vendita o la distribuzione, mette in commercio, vendita, noleggio, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo radio o televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o altro supporto per il quale è prescritto il contrassegno SIAE, privi del contrassegno o dotati di contrassegno contraffatto o alterato;
- e) ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato, in assenza di accordo con il legittimo distributore;
- f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuzione, vendita, concede in noleggio, cede a qualsiasi titolo, fa promozione commerciale, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso a un servizio criptato senza il pagamento del canone dovuto;
- f bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblica e vende o noleggia, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero prestazione di servizi aventi impiego commerciale o prevalente finalità di eludere efficaci misure tecnologiche di protezione ovvero progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di tali misure;
- g) abusivamente rimuove o altera informazioni elettroniche sul regime dei diritti di cui all'articolo 102-*quinquies*, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

La duplicazione abusiva di opere dell'ingegno può ricorrere se un soggetto dell'ente riproduce, trasmette o diffonde in pubblico in maniera abusiva opere o parti di opere intellettuali (ad es. letterarie, drammatiche, scientifiche, didattiche, musicali o multimediali, anche se inserite in opere collettive o composite o banche dati).

▪ **Omessa o falsa comunicazione alla SIAE dei dati di identificazione di supporti non soggetti a contrassegno (art. 171 septies L.A.)**

Punisce i produttori o importatori di supporti, non soggetti al contrassegno SIAE per la protezione del diritto d'autore, i quali non comunicano alla SIAE stessa, entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione, i dati necessari alla univoca identificazione dei supporti medesimi o comunicano falsamente di aver assolto agli obblighi previsti dall'art. 181-bis c. 2 L.A.

▪ **Produzione, vendita, importazione, promozione, installazione, modifica, utilizzo di apparati per la decodificazione di trasmissione audiovisive (art. 171 octies L.A.)**

Punisce chi fraudolentemente produce, vende, importa, promuove, installa, modifica, utilizza per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato (es. SKY) effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

Il reato di cui all'art. 640 ter c.p. *frode informatica in danno dello Stato o di altro ente pubblico*, richiamato all'art. 24 D.Lgs 231/01, sarà trattato, nella presente Parte Speciale. Ciò in quanto, riguardando sistemi informatici o telematici, o dati, informazioni o programmi in essi contenuti, risulta evitabile con modalità proprie dei delitti informatici, come si vedrà in seguito.

10.1.1 Esclusioni

Per quanto riguarda i reati informatici, si sono esclusi i reati previsti dall'art. 615 ter e dall'art. 615 quinquies, in quanto al momento non ci sono competenze specifiche all'interno dell'Ente per la commissione degli stessi, così come quelli previsti dall'art. 617 quater, dall'art. 617 quinquies, dall'art. 635 ter, dall'art. 635 quinquies per il medesimo motivo. È stato escluso anche il reato previsto dall'art. 640 quinquies c.p. perché trattasi di reato proprio, il cui soggetto attivo può essere solamente chi presta servizi di certificazione di firma elettronica.

Per quanto riguarda i delitti in violazione del diritto d'autore, gli unici reati considerati, in quanto ipoteticamente rilevanti per l'Ente, sono quelli previsti all'art. 171 comma 1 lettera a) bis, comma 3 e all'art. 171 bis della Legge sul Diritto d'Autore (Legge 22 aprile 1941 n. 633), ossia la protezione dell'opera di ingegno, anche non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, nonché protezione del software e delle banche dati; e l'art. 171 ter.

10.1.2 Individuazione dei processi sensibili

Nell'analisi compiuta al fine della predisposizione del presente Modello si è potuto accertare che la maggior parte degli ambiti dell'attività sociale è interessata dall'utilizzo dei sistemi informatici e, pertanto, i reati sopra richiamati potrebbero astrattamente essere oggetto di condotta specifica e/o costituire il mezzo per addivenire al compimento di altre fattispecie rilevanti ai sensi del D.Lgs 231/01.

Ne risulta che tutte le attività nelle quali si utilizzino i Sistemi Informatici di Ter Servizi, il servizio di posta elettronica e l'accesso ad Internet, sono da considerarsi Processi sensibili.

Nell'individuazione dei presidi specifici per i reati di cui alla presente parte speciale, sono state analizzate principalmente le seguenti attività:

- gestione dei Sistemi Informativi e sito web;
- utilizzo del certificato qualificato/firma digitale;
- utilizzo della casella di posta elettronica certificata aziendale;
- utilizzo di software e banche dati.

10.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO

La presente parte speciale si applica a tutte le funzioni che utilizzino i sistemi informatici, quindi a chiunque sia definito Utente ai sensi del Regolamento per l'utilizzo dei sistemi informatici, nonché a coloro che più specificatamente gestiscano gli stessi, quindi:

- tutte le funzioni che gestiscono la pec aziendale ed a coloro che utilizzano firme digitali;
- tutte le funzioni che utilizzano la posta elettronica con intestazione personale;
- tutte le funzioni deputate alla progettazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni.

Nell'espletamento delle rispettive attività/funzioni, oltre a quanto indicato nel presente Modello, gli utenti del sistema informatico sono tenuti a rispettare il Codice Etico e i principi e le regole contenute nei seguenti documenti, che assurgono a presidi di controllo per i reati oggetto della presente parte speciale, nonché di quelli che possono essere commessi a mezzo dell'utilizzo dei sistemi informatici:

- Regolamento aziendale per l'utilizzo del sistema informatico consegnato a tutti i dipendenti e collaboratori. Tra gli altri è stato previsto l'obbligo di utilizzare il sistema solo per scopi lavorativi e non per commettere reati della tipologia evidenziata dalla norma.
- Adeguamento e rispetto della normativa sul Trattamento Dati e quindi del D.Lgs 196/03, con periodico aggiornamento della documentazione relativa e controllo sul corretto adempimento degli obblighi ivi previsti.
- Inserimento nelle schede di partecipazione ai corsi della richiesta di consenso all'utilizzo dei dati sia per le finalità del corso sia per l'inoltro di comunicazioni a fini commerciali.
- Formazione del personale sia sull'utilizzo dei sistemi informatici, che negli specifici obblighi ex D.Lgs 196/03;
- Formalizzazione dei contratti per la manutenzione di reti telematiche/HW.

In particolare, in seguito all'attività di risk assessment, effettuata dall'Ente, sono state individuate le seguenti attività aziendali considerate a rischio.

10.2.1 Utilizzo del sistema informatico e del sito web

Il sistema informatico di Ter-Servizi è inserito nel più ampio sistema gestito dall'Ascom - Unione Provinciale, che si colloca nello stesso stabile e mette a disposizione delle varie realtà ad essa collegate sia la connettività esterna che le funzioni di sicurezza e backup.

Ter-Servizi mantiene la proprietà delle apparecchiature in uso ai propri dipendenti e collaboratori, e del software in esse contenuto, ma queste si inseriscono nella rete cablata gestita dal CED dell'Unione, e vengono completate dai servizi di hosting del sito e di gestione della posta elettronica che sono erogati dall'Unione.

Vi è quindi, fra l'Unione e Ter-Servizi, un contratto che specifica nel dettaglio le specifiche competenze, i servizi garantiti dal CED dell'Unione, i limiti di responsabilità fra i due soggetti.

Al fine di regolamentare l'utilizzo del sistema informatico è stato predisposto il Regolamento aziendale per l'utilizzo del sistema informatico il quale prescrive una serie di norme di comportamento che gli utenti devono tenere nell'utilizzo quotidiano delle apparecchiature.

Tale documento, destinato ai dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (c.d. *Utenti*), disciplina le seguenti attività:

- Utilizzo del Personal Computer
- Gestione delle Credenziali di autenticazione
- Utilizzo della rete di Ter-Servizi
- Utilizzo dei supporti esterni di memorizzazione
- Utilizzo di Smartphone e PC portatili
- Uso della posta elettronica
- Uso della rete Internet e dei relativi servizi

L'utilizzo delle postazioni può avvenire solamente tramite credenziali di autenticazione, la cui gestione viene compiuta conformemente a quanto stabilita dal Regolamento per l'utilizzo dei sistemi informatici.

I software utilizzati sono tutti autorizzati e muniti di licenza.

Anche per quelli forniti dall'Unione vi è garanzia contrattuale di rispetto delle licenze d'uso.

Le funzioni di analisi e manutenzione del sistema informatico sono state attribuite, giusta delega-lettere di incarico, all'amministratore di sistema dell'Unione Provinciale.

I poteri per l'espletamento delle sue funzioni sono descritti nell'apposita lettera di incarico, che richiama quella rilasciata dall'Unione al proprio AdS.

Chiunque venga a conoscenza di comportamenti contrari a quanto prescritto nel Regolamento suddetto, nel presente Modello o nella procedura richiamata, dovrà informarne l'OdV.

10.2.2 Utilizzo della firma digitale

Il certificato qualificato/firma digitale, intestato all'Amministratore Delegato, è utilizzato esclusivamente dall'Amministratore Delegato stesso o dal funzionario di TER-Servizi munito di apposita delega e formato sul valore giuridico della firma digitale.

10.2.3 Utilizzo di software e banche dati

Per quanto riguarda le modalità di utilizzo di software e di banche dati gli Utenti sono tenuti al rispetto del Regolamento per l'utilizzo dei sistemi informatici che è stato distribuito ad ogni Utente e sul quale viene fatta formazione da parte di Ter Servizi.

Nel caso di dubbio sull'utilizzo di software e banche dati l'Utente è invitato a rivolgersi all'Amministratore di Sistema.

10.3 FLUSSI INFORMATIVI VERSO L'ODV

I flussi sono regolati secondo quanto previsto al paragrafo 6.4 della parte Generale del presente modello.

PARTE SPECIALE C I REATI SOCIETARI

11. PARTE SPECIALE C - I REATI SOCIETARI

11.1 FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati societari.

Si indicano brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 all'art. 25 ter, rimandandosi al testo del decreto, a quello del Codice Penale nonché a quelli del Codice Civile per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Codice Penale.

I reati societari vengono raggruppati, per maggiore chiarezza, in cinque gruppi.

FALSITA' IN COMUNICAZIONI, PROSPETTI E RELAZIONI

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

Tale reato si configura nel caso in cui nell'intento di ingannare i soci o il pubblico ed al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero vengano ivi omesse informazioni sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene la cui comunicazione è imposta dalla legge, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione.

La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria dell'Ente o del gruppo al quale essa appartiene.

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

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscano in misura non superiore al 10 per cento da quella corretta.

- **Fatti di lieve entità (art. 2621-bis c.c.)**

Tale ipotesi di reato si configura laddove i fatti di cui all'art. 2621 c.c. siano di lieve entità, salvo che costituiscano più grave reato.

- **False comunicazioni sociali delle società quotate (art. 2622 c.c.)**

Tale ipotesi di reato si configura nel caso in cui, nell'intento di conseguire per sé o per altri un ingiusto profitto, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, espongano nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero ovvero omettano fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società o del gruppo al quale essa appartiene, in modo idoneo ad indurre altri in errore.

Detta previsione si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dall'Ente per conto terzi.

Si precisa, inoltre, che:

- le fattispecie penali indicate richiedono che le informazioni false o omesse siano tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria dell'Ente o del gruppo al quale essa appartiene,
- sussiste la responsabilità dell'ente anche qualora le informazioni false o omesse riguardino beni posseduti o amministrati dall'Ente per conto di terzi,
- detti reati sono cd. "propri", cioè commissibili solamente da soggetti qualificati, che sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

- **Falso in prospetto (art. 2623 c.c.)**

Tale ipotesi di reato è stata abrogata dall'art. 342 della Legge 28 dicembre 2005, n.262; tuttavia, l'art. 25 ter del Decreto non è stato aggiornato, ma continua a fare rinvio a detto articolo del codice civile.

La Dottrina dominante ha rilevato che l'art. 173 bis del TUF (d.lgs. 24 febbraio 1998, n.58) prevede un'ipotesi di reato più che coincidente, ma, tuttavia, considerando il rinvio dell'art. 25 ter del Decreto all'art. 2623 c.c. come "recettizio", ritiene che non si possa parlare di continuità normativa tra le due ipotesi di reato e che la responsabilità amministrativa dell'ente sia venuta meno.

▪ **Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.)**

Tale ipotesi di reato è stata abrogata dall'art. 37, comma 34 del D.lgs. 27 febbraio 2010, n. 39; tuttavia, l'art. 25 ter del Decreto non è stato aggiornato, ma continua a fare rinvio a detto articolo del codice civile.

La Dottrina dominante ha rilevato che l'art. 27 del suddetto decreto prevede un'ipotesi di reato più che coincidente, ma, tuttavia, considerando il rinvio dell'art. 25 ter del Decreto all'art. 2624 c.c. come "recettizio", ritiene che non si possa parlare di continuità normativa tra le due ipotesi di reato e che la responsabilità amministrativa dell'ente sia venuta meno. Sul punto è intervenuta la Suprema Corte, a sezioni unite, (Cass. Pen. Sez. Un., 23 giugno 2011, n. 34476) che ha rilevato come non sia possibile applicare l'art. 27 in relazione alla responsabilità amministrativa da reato degli enti.

TUTELA PENALE DEL CAPITALE SOCIALE

Sono tutti reati cd. "propri", perché ne possono essere soggetti attivi unicamente quelli aventi la qualifica indicati dalla norma incriminatrice.

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

Tale ipotesi di reato consiste nel procedere, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.

I soggetti attivi del reato possono essere solamente le persone qualificate dalla norma incriminatrice: gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Si evidenzia, però, che resta la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

▪ **Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)**

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite.

Si fa presente che:

- la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato;
- i soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario.

Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

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

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto od alla sottoscrizione di azioni o quote emesse dalla società (o dalla società

controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

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;
- i soggetti attivi del reato sono gli amministratori.

E' configurabile, tuttavia, una responsabilità a titolo di concorso ex art. 110 c.p. degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

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

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

Si fa presente che:

- il risarcimento del danno ai creditori prima del giudizio estingue il reato;
- il reato è punibile a querela di parte;
- i soggetti attivi del reato sono solo gli amministratori.

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

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

Soggetti attivi del reato sono gli amministratori ed i soci conferenti.

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

Tale ipotesi di reato consiste nella ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si fa presente che:

- il reato è perseguibile a querela della persona offesa;
- il risarcimento del danno ai creditori prima del giudizio estingue il reato.
- i soggetti attivi del reato sono esclusivamente i liquidatori.

TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETA'

▪ **Impedito controllo (art. 2625, 2° comma c.c.)**

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

Le sanzioni sono maggiorate qualora la condotta abbia cagionato un danno ai soci ed il reato è punibile solo a querela di parte.

E' un reato proprio, perché può essere commesso esclusivamente dagli amministratori.

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

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

Il reato può essere commesso da "chiunque" ponga in essere la condotta descritta dalla norma incriminatrice.

▪ **Omessa comunicazione del conflitto di interesse (art. 2629-bis c.c.)**

Tale ipotesi di reato consiste nella violazione degli obblighi previsti dall'art. 2391, 1° co. cod. civ. da parte dell'amministratore di una società con titoli quotati in mercati

regolamentati italiani o di altro Stato dell'Unione europea (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione derivano danni all'Ente od a terzi.

Si rileva che a norma dell'art. 2391, 1° comma c.c. gli amministratori delle società per azioni devono dare notizia agli altri amministratori e al collegio sindacale d'ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione dell'Associazione, precisandone la natura, i termini, l'origine e la portata, mentre gli amministratori delegati devono, altresì, astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale. L'amministratore unico deve darne notizia anche alla prima assemblea utile.

TUTELA PENALE CONTRO LE FRODI

▪ **Aggiotaggio (art. 2637 c.c.)**

Tale ipotesi di reato consiste nel diffondere notizie false ovvero nel realizzare operazioni simulate o altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero nell'incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Questo reato può essere commesso da "chiunque" ponga in essere la condotta descritta dalla norma incriminatrice.

TUTELA PENALE CONTRO L'OSTACOLO ALL'ATTIVITA' DI VIGILANZA PUBBLICA

▪ **Ostacolo all'esercizio dell'attività delle autorità pubbliche di vigilanza (art. 2638 c.c.)**

Tale ipotesi di reato si configura nel caso in cui attraverso comunicazioni non rispondenti al vero ovvero occultando, in tutto o in parte, con altri mezzi fraudolenti, fatti e circostanze sulla situazione economica, patrimoniale o finanziaria della società, si ostacoli l'attività di vigilanza della autorità pubbliche preposte.

Il reato è configurabile solamente qualora la Società sia sottoposta al controllo di autorità pubbliche di vigilanza (ad esempio Corte dei conti, Commissione Europea, Regione, Provincia e comune) ed abbia, per legge, l'obbligo di informativa nei confronti dei soci che siano Enti pubblici.

Con la legge "Anticorruzione" n. 190 del 6.11.2012, pubblicata in G.U. il 13.11.2012, il legislatore italiano ha dato attuazione alle disposizioni contenute nella Convenzione di Strasburgo del 27.1.1999, ratificata con la **L. n. 110 del 28.6.2012.**

La L. n. 190 del 2012, intitolata "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", è intervenuta, sul fronte della repressione, anche con l'introduzione del seguente nuovo reato:

▪ **Corruzione tra privati (art. 2635 comma 3 c.c.)**

Il reato consiste nel dare o promettere denaro o altra utilità ad:

- amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori,
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati sopra,

quando, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, questi compiano od omettano atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento all'Ente.

11.1.1 Esclusioni

Dopo l'analisi delle tipologie dei reati societari, si è ritenuto di escluderne la possibilità di accadimento per alcuni, in quanto non risultano compatibili con la società per ragioni giuridiche.

Per altri quali l'Impedito Controllo 2625 c.c., illecite operazioni sulle azioni 2628 c.c., Operazioni in pregiudizio dei creditori art. 2629 c.c., Illecita influenza sull'Assemblea 2636 C.C. si ritiene il rischio molto basso alla luce delle dimensioni, della tipologia e della struttura organizzativa dell'Ente, e per la realtà stessa della società, la quale pur essendo a scopo di lucro, riveste una "mission" particolare che non è quella del profitto, bensì del servizio al cittadino e all'impresa ed è partecipata al 60% da realtà quale l'Unione delle Imprese e delle Attività Professionali del lavoro; in linea di principio, più rilevanti per l'attività i reati di false comunicazioni sociali di cui all'art. 2621 c.c., e di corruzione tra privati 2635 co 3 c.c.

Reati esclusi	Motivazione
False comunicazioni sociali delle società quotate (art. 2622 c.c.)	L'Ente non è società quotata
Falso in prospetto (art. 2623 c.c.) - confluito nell'art. 173 TUF	Articolo abrogato. Anche se si ritenesse applicabile l'art. 173 Tuf, comunque nel caso concreto non sarebbe configurabile.
Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.)	Articolo Abrogato
Indebita restituzione dei conferimenti (art. 2626 c.c.)	Reati propri dell'amministratore/ non ci sono utili da ripartire e non è ipotizzabile una restituzione dei conferimenti
Indebita ripartizione degli utili o delle riserve (art. 2627 c.c.)	
Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)	L'Ente non è in liquidazione/ reato proprio del liquidatore
Aggiotaggio (art. 2637 c.c.)	Reato non realizzabile nella realtà aziendale in esame perché la società non è operante sul mercato
Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)	Reato non realizzabile in quanto non sottoposto alla sorveglianza di autorità pubblica di vigilanza

11.1.2 Individuazione dei processi sensibili

A conclusione dell'attività di valutazione condotta al fine della predisposizione del presente Modello, sono state identificate le seguenti aree sensibili:

- Redazione del bilancio e gestione del patrimonio;
- Gestione e Funzionamento dell'Assemblea;
- Tesoreria.

11.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO

Processo di definizione del bilancio – Gestione del patrimonio - Operazioni con i finanziamenti ricevuti

La peculiarità dei reati che possono astrattamente considerarsi nella presente parte è quella di essere reati propri degli amministratori (con l'esclusione degli art. 2636 c.c. e 2635 comma 3 c.c.).

Ciò comporta che, per quanto attiene il processo di definizione del bilancio una attenta e accurata gestione dei dati contabili e di bilancio, attraverso il sistema informatico e la

tracciabilità di tutte le operazioni di acquisto, vendita e quant'altro costituisca presidio fondamentale atto a prevenire la commissione dei su descritti reati-presupposto.

L'area sensibile in esame fa capo al Consiglio di Amministrazione, alla dipendente amministrativa e al commercialista esterno che collabora per la predisposizione e redazione del bilancio e calcolo delle imposte.

Per i pagamenti e gli acquisti, ci si richiama comunque ai presidi indicati nella Parte Speciale A del Modello.

Al fine di prevenire il reato di corruzione tra privati, si richiamano i presidi specifici e generali già elencati nella parte speciale A.

Quali presidi comuni a tutti i reati societari, sono le seguenti regole di condotta che hanno quali destinatari gli Amministratori, i collaboratori e i consulenti esterni o comunque coloro che partecipano alla redazione dei documenti contabili societari, nonché tutte le persone sottoposte alla loro direzione o vigilanza, nonché i consulenti esterni che operino nelle aree interessate:

- Divieto a carico degli Organi dell'Ente (e dei Dipendenti e Consulenti nella misura necessaria alla funzione dagli stessi) di porre in essere, istigare, 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 considerate dall'art. 25 ter del D.Lgs. 231/2001.
- Obbligo di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi, una informazione completa, veritiera e corretta sulla situazione economica, patrimoniale e finanziaria dell'Ente. Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:
 - rappresentare o trasmettere dati falsi, lacunosi, parziali, o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria dell'Ente;
 - omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- Obbligo di tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione, registrazione, documentazione ed illustrazione dei dati e delle informazioni necessarie per consentire ai soci ed ai finanziatori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'Ente e sull'evoluzione della sua attività; nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:
 - alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi eventualmente emessi;
 - illustrare i dati e le informazioni in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria di Ter-Servizi e sull'evoluzione della sua attività;
- Obbligo di osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere; nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:
 - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
 - ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;

- acquistare o sottoscrivere azioni dell'Associazione o di Società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumento fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- Obbligo di assicurare il regolare funzionamento dell'Associazione e degli Organi associativi, garantendo ed agevolando ogni forma di controllo interno sulla gestione dell'Ente previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare. Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:
 - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del collegio dei revisori;
 - determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

11.3 FLUSSI INFORMATIVI VERSO L'ODV

I flussi sono regolati secondo quanto previsto al paragrafo 6.4 della parte Generale del presente modello.

PARTE SPECIALE D I REATI DI RICETTAZIONE E RICICLAGGIO

12. PARTE SPECIALE D - I REATI DI RICETTAZIONE E RICICLAGGIO

12.1 FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati di ricettazione, riciclaggio ed impiego di denaro beni e utilità di provenienza illecita. Si indicano brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 all'art. 25-octies, richiamante i reati di cui agli artt. 648, 648-bis, 648-ter e 648-ter1 c.p., rimandandosi al testo del Decreto e a quello del Codice Penale per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Codice Penale.

▪ Ricettazione (art. 648 c.p.)

Il reato si configura quando l'agente, fuori dei casi di concorso nel reato presupposto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto o, comunque, si intromette per farle acquistare, ricevere od occultare, al fine di procurare per sé o per altri un profitto.

Presupposto necessario della ricettazione è che anteriormente sia stato commesso un altro delitto, non rilevando che esso sia giudizialmente accertato (cd. reato presupposto).

▪ Riciclaggio (art. 648-bis c.p.)

Il reato si configura quando l'agente, fuori dei casi di concorso nel reato presupposto, 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 la identificazione della loro provenienza delittuosa.

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

▪ Impiego di denaro beni e utilità di provenienza illecita (art. 648-ter c.p.)

Il reato si configura quando la condotta illecita di impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, ove l'autore non abbia concorso alla realizzazione del reato presupposto (ad es. furto, reati tributari, reati di falso, ecc.), non sia riconducibile alle ipotesi di cui all'art 648 (ricettazione) o all'art. 648 bis (riciclaggio).

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

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

Il reato si configura nel caso un soggetto, avendo commesso o concorso a commettere un delitto non colposo, impiega o sostituisce o trasferisce in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

Premesso che presupposto comune delle fattispecie incriminatrici previste dagli articoli sopra menzionati è quello costituito dalla provenienza da delitto del denaro e dell'altrui utilità di cui l'agente è venuto a disporre, dette fattispecie si distinguono, sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della suindicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda e la terza richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto alla terza, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche o finanziarie.

La normativa italiana in tema di prevenzione dei suddetti reati per ostacolare le pratiche di riciclaggio vieta, tra l'altro, l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi.

Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal Decreto Antiriciclaggio, che ha in parte abrogato e sostituito la legge del 5 luglio 1991 n. 197.

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

1. la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione sia pari o superiori a Euro 1.000,00. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.;
2. l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti destinatari del Decreto Antiriciclaggio (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi;
3. l'obbligo da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;
4. l'obbligo di segnalazione da parte di alcuni soggetti (elencati agli artt. 10, comma 2, 11, 12, 13 e 14 del Decreto Antiriciclaggio) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.

I soggetti sottoposti agli obblighi di cui ai n. 2, 3, 4, sono:

1. gli intermediari finanziari e gli altri soggetti esercenti attività finanziaria. Tra tali soggetti figurano, ad esempio banche, Poste Italiane, società di intermediazione mobiliare, società di gestione del risparmio (SGR), società di investimento a capitale variabile (SICAV);
2. i professionisti, tra i quali si indicano i soggetti iscritti nell'albo dei ragionieri e periti commerciali; i notai e gli avvocati quando, in nome e per conto dei loro clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i loro clienti in determinate operazioni;
3. i revisori contabili;
4. altri soggetti, intesi quali operatori che svolgono alcune attività il cui esercizio resta subordinato al possesso delle licenze, autorizzazioni, iscrizioni in albi o registri, ovvero alla preventiva dichiarazione di inizio di attività richieste dalle norme. Tra le attività si indicano recupero di crediti per conto terzi; trasporto di denaro contante; gestione di case da gioco; offerta, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro.

12.1.1 Esclusioni

Anche se non vengono escluse le fattispecie previste dalla presente Parte Speciale, il rischio viene considerato basso, stanti le prassi consolidate all'interno della Società, e alla luce delle dimensioni, della tipologia e della struttura organizzativa dell'Ente, e per la realtà stessa della società, la quale pur essendo a scopo di lucro, riveste una "mission" particolare che non è quella del profitto, bensì del servizio al cittadino e all'impresa ed è partecipata al 60% da realtà quale l'Unione delle Imprese e delle Attività Professionali del lavoro.

12.1.2 Individuazione dei processi sensibili

I principali Processi Sensibili, che potrebbero essere astrattamente interessati dalla commissione dei reati qui analizzati, anche con riferimento alla distrazione di fondi per la commissione di reati altrimenti rilevanti, sono i seguenti:

- Gestione della liquidità di cassa.

12.2 PRINCIPI DI COMPORTAMENTO – ELEMENTI ATTUATIVI DEL MODELLO

Presupposto comune dei reati della presente parte speciale è la consapevolezza della provenienza illecita del denaro o delle cose acquistate o ricevute.

Sussiste un presidio generale, che limita l'utilizzo dei contanti nei pagamenti, essendo questi richiesti unicamente per bonifico/assegno/POS.

Gli incassi per cassa hanno comunque un massimo accettabile di 500,00 Euro, ben al di sotto della soglia prevista per legge.

E' poi garantita la tracciabilità di tutte le entrate e le uscite, venendo tenuto un prospetto di riconciliazione cassa con tutte le movimentazioni di denaro e i soggetti che le hanno effettuate.

Alle entrate di denaro, anche in contanti, deve sempre corrispondere una fattura o uno scontrino.

I soggetti che pagano in contanti i corsi devono esibire il documento d'identità, che viene registrato.

Anche le uscite per cassa sono tutte documentate.

Presidi comuni a tutte le attività sensibili sono i seguenti principi fatti propri da Ter-Servizi e trasmessi a tutti i soggetti coinvolti in esse:

- divieto di ricevere od occultare denaro o cose provenienti da un qualsiasi delitto nel caso in cui utilizzando la normale diligenza professionale sarebbe stato possibile individuare la provenienza illecita di quanto ricevuto. Costituiscono esempi di utilizzo di una normale diligenza professionale la verifica nelle operazioni di acquisto di beni che il prezzo applicato non sia sproporzionato rispetto ai valori medi di mercato, la verifica della regolarità dei pagamenti a fornitori, con riferimento alla piena coincidenza tra destinatari dei pagamenti e controparti effettivamente coinvolte nelle transazioni;

- divieto di sostituire o trasferire denaro, beni o altre utilità provenienti da delitto non colposo nel compimento di atti negoziali oppure in altre operazioni in modo da ostacolare l'identificazione della loro provenienza delittuosa;
- divieto di impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto nel caso in cui utilizzando la normale diligenza professionale sarebbe stato possibile individuare la provenienza illecita di quanto ricevuto.

12.3 FLUSSI INFORMATIVI VERSO L'ODV

I flussi sono regolati secondo quanto previsto al paragrafo 6.4 della parte Generale del presente modello.

**PARTE SPECIALE E
I REATI DI OMICIDIO COLPOSO E LESIONI
COLPOSE GRAVI O GRAVISSIME IN
VIOLAZIONE DELLE NORME
ANTINFORTUNISTICHE E SULLA TUTELA
DELL'IGIENE E DELLA SALUTE SUL LAVORO**

13. PARTE SPECIALE E - I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

13.1 FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati di omicidio colposo e di lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. Si indicano brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 all'art. 25 *septies*, rimandandosi al testo del decreto e a quello del Codice Penale per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Cod. Pen.

▪ Omicidio colposo (art. 589 c.p.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa la morte di altro soggetto.

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

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

Ai sensi del comma 1 dell'art. 583 c.p., la lesione è considerata grave quando 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; ovvero, se il fatto produce l'indebolimento permanente di un senso o di un organo.

Ai sensi del comma 2 dell'art. 583 c.p., la lesione è considerata, invece, gravissima se dal fatto deriva una malattia certamente o probabilmente insanabile; la perdita di un senso; la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; la deformazione, ovvero lo sfregio permanente del viso.

13.1.1 Esclusioni

Non si rilevano esclusioni fra i reati di cui alla presente parte speciale.

13.1.2 Individuazione dei processi sensibili

Tutti i processi societari possono essere ritenuti sensibili in relazione al verificarsi dei reati in esame. L'evento infortunistico dal quale possano scaturire le lesioni gravi o gravissime, o l'omicidio colposo, può infatti avvenire in ogni area, fase lavorativa, momento della giornata, pur se con livelli di rischio ragionevolmente bassi, alla luce della tipologia di attività svolta da Ter-Servizi.

Risulta quindi superfluo identificare più in dettaglio ambiti specifici di rischio, dovendo comunque inglobare tutta l'attività sociale.

13.2 PRINCIPI DI COMPORTAMENTO NELL'AMBITO DELLE ATTIVITÀ A RISCHIO - ELEMENTI ATTUATIVI DEL MODELLO

La gestione della Sicurezza e Salute negli ambienti di lavoro è priorità assoluta e principio irrinunciabile per l'Ente, a tutti i livelli decisionali ed operativi.

Ter-Servizi, al fine di garantire la prevenzione degli infortuni e la tutela della salute dei lavoratori ha nominato un Datore di lavoro per la sicurezza, ed un RSPP; ha effettuato la valutazione dei rischi connessi con l'attività svolta o comunque con il luogo di lavoro; ha provveduto alla formazione dei dipendenti/collaboratori in materia di sicurezza e ha nominato un RLS.

Il RSPP provvede, pertanto, a monitorare tutte le attività di prevenzione dell'Ente, stilando anche un verbale periodico in cui dà evidenza delle azioni svolte a favore di Ter Servizi e degli adempimenti/suggerimenti da porre in essere. In specifico, le attività del RSPP si possono riassumere in:

- Tenuta sotto controllo dell'evoluzione normativa, adeguamento tempestivo e continuo ad essa, in tutti gli aspetti;
- Monitoraggio e controllo dei processi, della struttura, dei fattori di rischio;
- Valutazione della correttezza delle soluzioni di prevenzione adottate in azienda;
- Informazione puntuale e completa ai lavoratori, nonché suggerimenti per azioni di formazione e aggiornamento degli stessi, al fine di accrescere continuamente la consapevolezza e la partecipazione di tutti nella riduzione dei rischi e prevenzione degli infortuni;

La reale ed efficace attuazione delle misure di prevenzione, l'elevato livello di formazione e la continua opera di controllo e verifica da parte del Datore di Lavoro e dei Preposti preposti, le azioni di sorveglianza dell'OdV, sono gli elementi fondanti del Modello in relazione ai reati considerati.

13.3 INFORMATIVI VERSO L'ODV

I flussi sono regolati secondo quanto previsto al paragrafo 6.4 della parte Generale del presente modello.