27 Luglio 2015

Modello di Organizzazione, Gestione e Controllo di Teleippica S.r.l. ai fini del D.Lgs. 231/01

Indice

DEFINIZIONI

Le parole e le espressioni contraddistinte nel presente documento con lettera iniziale maiuscola hanno il significato, di seguito, specificato:

"**Aree a Rischio**":	le Aree di attività ed i processi aziendali a rischio diretto o strumentale alla commissione dei reati;
"**Controlli Aziendali**":	il sistema di deleghe, procure, procedure e controlli interni aventi quale finalità quella di garantire un'adeguata trasparenza e conoscibilità dei processi decisionali, nonché i comportamenti che devono essere tenuti dai Soggetti Apicali e dai Soggetti Sottoposti, operanti nelle aree aziendali;
"**Destinatari**":	Organi Sociali, Personale - Soggetti Apicali e i Soggetti Sottoposti - ed i Terzi;
"**D. Lgs 231/2001**" o il "**Decreto**":	il Decreto Legislativo 8 giugno 2001, n. 231;
"**Documento**":	il presente Documento;
"**Linee Guida**":	le linee guida, approvate da Confindustria in data 7 marzo 2002 e successivamente aggiornate, per la costruzione dei Modelli di organizzazione gestione e controllo *ex* D.Lgs. n. 231/01;
"**Modello**":	il presente Documento, le Parti Speciali (A, B, B1, C, D, E, F), il Sistema Sanzionatorio, il Codice Etico, ed i Controlli Aziendali. Ne consegue che, con il termine Modello deve intendersi non solo il presente Documento, ma altresì tutti gli ulteriori documenti che verranno successivamente adottati;
"**OdV**" o "**Organismo di Vigilanza**":	l'organismo nominato ai sensi dell'art. 6 D.Lgs. n. 231/2001 ed avente i compiti ivi indicati;
"**Reati contro la Pubblica Amministrazione**":	i reati *ex* artt. 24 e 25 del D.Lgs. n. 231/01;
"**Delitti informatici"**:	i reati *ex* art. 24-*bis* del D.Lgs. n. 231/01;
"**Reati Societari**":	i reati *ex* art. 25-*ter* del D.Lgs. n. 231/2001;
"**Reati sulla Salute e Sicurezza sul Lavoro**":	i reati *ex* art. 25-*septies* del D.Lgs. n. 231/2001;
"**Reati di Ricettazione, Riciclaggio e Impiego di denaro, beni o utilità di provenienza illecita, nonché Autoriciclaggio**":	i reati *ex* art. 25-*octies* del D.Lgs. n. 231/2001;

"Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria":	i reati *e*x art. 25-*decies* del D.Lgs. n. 231/2001;
"Reati Ambientali"	i reati ex art. 25-*undecies* del D.Lgs. n.231/2001;
"Delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare"	i reati ex art. 25-*duodecies* del D.Lgs. n.231/2001;
"**Codice Etico"**:	il documento nel quale sono definiti i principi fondamentali a cui Teleippica S.r.l. si ispira ed intende uniformare la propria attività;
"Archivio documentale":	l'archivio documentale, accessibile ai Soggetti Apicali e Sottoposti, contenente i documenti connessi al presente Documento;
"**Società**":	Teleippica S.r.l.;
"**Sistema Sanzionatorio**":	il sistema disciplinare e il relativo meccanismo sanzionatorio da applicare in caso di violazione del Modello;
"**Soggetti Apicali**":	ai sensi dell'art. 5 del D.Lgs. n. 231/2001, le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo degli stessi;
"**Soggetti Sottoposti**":	ai sensi dell'art. 5 del D.Lgs. n. 231/2001, e sulla base dell'orientamento dottrinale prevalente, i soggetti dipendenti e non, sottoposti alla direzione o alla vigilanza di uno dei Soggetti Apicali;
"**Terzi**"	Tutti i soggetti esterni: i consulenti, le controparti contrattuali, i fornitori, i clienti, i partner (laddove presenti), nonché tutti coloro che, pur esterni alla società, operino, direttamente o indirettamente, per Teleippica S.r.l..

1 LA RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI

1.1. Il regime giuridico della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito anche indicato come il "Decreto"), avente ad oggetto la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" ha introdotto nell'ordinamento italiano la responsabilità degli enti.

Il Decreto ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali in precedenza sottoscritte dall'Italia, come le Convenzioni di Bruxelles del 26 luglio 1995 e del 26 maggio 1997 sulla tutela degli interessi finanziari della Unione Europea e sulla lotta alla corruzione di funzionari pubblici sia della Unione Europea che degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il D.Lgs. n. 231/2001 si inserisce dunque in un contesto di attuazione degli obblighi internazionali e – allineandosi con i sistemi normativi di molti Paesi dell'Europa – istituisce la responsabilità della *societas*, considerata quale autonomo centro di interessi e di rapporti giuridici, punto di riferimento di precetti di varia natura, e matrice di decisioni ed attività dei soggetti che operano in nome, per conto o comunque nell'interesse dell'ente.

L'istituzione della responsabilità amministrativa delle società nasce dalla considerazione empirica che frequentemente le condotte illecite commesse all'interno dell'impresa, lungi dal conseguire ad un'iniziativa privata del singolo, rientrano piuttosto nell'ambito di una diffusa *politica aziendale* e conseguono a decisioni di vertice dell'ente medesimo.

Le disposizioni di cui al Decreto si applicano, per espressa previsione dell'art. 1 dello stesso, ai seguenti "soggetti" (qui di seguito gli "Enti"):

- ✓ *enti forniti di personalità giuridica;*
- ✓ *società e associazioni anche prive di personalità giuridica.*

Con riferimento alla natura della responsabilità amministrativa degli Enti ai sensi del Decreto, la Relazione illustrativa al Decreto medesimo ha sottolineato che si tratta di un "*tertium genus che coniuga i tratti essenziali del sistema penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle, ancor più ineludibili, della massima garanzia*".

La normativa in parola è frutto di una tecnica legislativa che, mutuando i principi propri dell'illecito penale e dell'illecito amministrativo, ha introdotto nel nostro ordinamento un sistema punitivo degli illeciti di impresa che va ad aggiungersi e ad integrarsi con gli apparati sanzionatori esistenti.

La responsabilità amministrativa dell'Ente è autonoma rispetto a quella della persona fisica che commette il reato: l'Ente, infatti, non è ritenuto esente da responsabilità anche qualora l'autore del reato non sia

stato identificato o non sia imputabile o qualora il reato si estingua per causa diversa dall'amnistia (art. 8 del Decreto).

In ogni caso, la responsabilità dell'Ente si aggiunge e non sostituisce quella della persona fisica autrice del reato.

Quanto ai soggetti, il Legislatore, all'art. 5 del D.Lgs. n. 231/2001, prevede la responsabilità dell'ente qualora il reato sia commesso da:

- *i "**Soggetti Apicali**";*
- *i "**Soggetti Sottoposti**".*

Può derivare una responsabilità ex D.Lgs. n. 231/2001 nei confronti della Società non solo per i reati commessi dai Soggetti Apicali e dai Soggetti Sottoposti, ma anche dai Terzi.

Ai fini dell'affermazione della responsabilità dell'ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'ente, il Legislatore impone inoltre l'accertamento della colpevolezza dell'ente. Siffatto requisito soggettivo si identifica con una *colpa da organizzazione*, intesa come violazione di adeguate regole di diligenza autoimposte dall'ente medesimo e volte a prevenire lo specifico rischio da reato.

1.2. I criteri di imputazione della responsabilità all'Ente e le esenzioni dalla responsabilità

Se è commesso uno dei reati-presupposto (illustrati al paragrafo 1.3 che segue), l'Ente è responsabile soltanto se si verificano certe condizioni, definite come criteri di imputazione del reato all'Ente e che si distinguono in "***oggettivi***" e "***soggettivi***".

La prima condizione oggettiva è che il reato-presupposto sia stato commesso da un soggetto legato all'Ente da un rapporto qualificato. L'art. 5 del Decreto, infatti, indica quali autori del reato:

- ***soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale o soggetti che esercitano di fatto la gestione ed il controllo dell'Ente*** *(cosiddetti Soggetti in posizione apicale o apicali);*

- ***soggetti sottoposti alla direzione o alla vigilanza di soggetti apicali*** *(cosiddetti Soggetti in posizione subordinata o sottoposti, personale non dirigente).*

La seconda condizione oggettiva è che la condotta illecita sia stata realizzata dai soggetti suindicati "*nell'interesse o a vantaggio della società*" (art. 5, co. 1 del Decreto):

- ✓ l'"***interesse***" sussiste quando l'autore del reato ha agito con l'intento di favorire l'Ente, indipendentemente dalla circostanza che poi tale obiettivo sia stato raggiunto;

- ✓ il "***vantaggio***" sussiste quando l'Ente ha tratto, o avrebbe potuto trarre, dal reato un risultato positivo, non necessariamente di natura economica.

Per espressa volontà del Legislatore, l'Ente non risponde nell'ipotesi in cui i Soggetti apicali o i Soggetti in posizione subordinata hanno agito "*nell'interesse esclusivo proprio o di terzi*" (art. 5, co. 2 del Decreto).

Il criterio dell'"*interesse o vantaggio*", coerente con la direzione della volontà propria dei delitti dolosi, è di per sé non compatibile con la struttura colposa dei reati presupposto previsti dall'art. 25-septies del Decreto (omicidio e lesioni colpose).

In tali ultime fattispecie, la componente colposa (che implica la mancanza della volontà) porterebbe ad escludere che si possa configurare il reato presupposto nell'interesse dell'ente. Tuttavia, la tesi interpretativa maggiormente accreditata ritiene come criterio di ascrizione dei reati colposi la circostanza che l'inosservanza della normativa antinfortunistica costituisca un oggettivo vantaggio per l'ente (quanto meno sotto il profilo dei minori costi derivanti dalla citata inosservanza). Risulta quindi chiaro che l'inosservanza della normativa antinfortunistica rechi un vantaggio all'ente.

Per quanto concerne i criteri soggettivi di imputazione del reato all'Ente, essi stabiliscono le condizioni in base alle quali il reato è "ascrivibile" all'Ente: affinché il reato non possa essere ad esso imputato sotto il profilo soggettivo, l'Ente deve dimostrare di avere fatto tutto quanto in suo potere per organizzarsi, gestirsi e controllare che nell'esercizio dell'attività di impresa non possa essere commesso uno dei reati-presupposto tra quelli elencati nel Decreto.

Per questa ragione, il Decreto prevede che la responsabilità dell'Ente può essere esclusa qualora, prima della commissione del fatto:

- ✓ *siano predisposti ed attuati Modelli di Organizzazione e di Gestione idonei a prevenire la commissione dei reati;*
- ✓ *sia istituito un organo di controllo (Organismo di Vigilanza), con poteri di autonoma iniziativa con il compito di vigilare sul funzionamento dei modelli di organizzazione.*

Nell'ipotesi di reati commessi dai Soggetti in posizione apicale, il Legislatore ha previsto una presunzione di colpa per l'Ente, in considerazione del fatto che i soggetti apicali esprimono, rappresentano e concretizzano la politica gestionale dell'Ente stesso: la responsabilità dell'Ente è esclusa soltanto qualora quest'ultimo dimostri che il reato è stato commesso eludendo fraudolentemente il Modello di Organizzazione, Gestione e Controllo (qui di seguito il "Modello") esistente e che vi sia stato un insufficiente controllo da parte dell'Organismo di Vigilanza (qui di seguito "OdV"), appositamente incaricato di vigilare sul corretto funzionamento e sull'effettiva osservanza del Modello stesso (art. 6 del Decreto).[1] In queste ipotesi, dunque, il Decreto richiede una prova di estraneità dai fatti, poiché l'Ente deve provare un raggiro doloso del Modello da parte dei Soggetti apicali.

[1] Ai sensi dell'art. 6, co.1, D.Lgs. 231/2001, "*Se il reato è stato commesso dalle persone indicate nell'art 5, comma 1, lettera a)* [i soggetti apicali], *l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)*".

Nel caso di reato realizzato dal sottoposto, invece, si avrà la responsabilità dell'Ente soltanto qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza: in questa ipotesi l'esclusione della responsabilità dell'Ente è subordinata, in sostanza, alla adozione di protocolli comportamentali adeguati, per il tipo di organizzazione e di attività svolta, a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio (art. 7, co. 1 del Decreto).[2] Si tratta, in questo caso, di una vera e propria "*colpa di organizzazione*", poiché l'Ente ha indirettamente acconsentito alla commissione del reato, non presidiando adeguatamente le attività e i soggetti a rischio di commissione di un reato-presupposto.

[2] Ai sensi dell'art. 7, co.1, D.Lgs. 231/2001, "*Nel caso previsto dall'art. 5, comma 1, lettera b)* [i soggetti in posizione subordinata], *l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza*".

1.3.Illeciti e reati che determinano la responsabilità amministrativa

Originariamente prevista per i Reati contro la Pubblica Amministrazione o contro il patrimonio della Pubblica Amministrazione, la responsabilità dell'ente è stata estesa – per effetto dei provvedimenti normativi successivi al D.Lgs. n. 231/2001 – a numerosi altri reati e illeciti amministrativi.

Segnatamente, la responsabilità amministrativa degli enti può conseguire dai seguenti reati/illeciti amministrativi:

i) Reati contro la Pubblica Amministrazione (articoli 24 e 25 del D.Lgs. n. 231/01);
ii) Delitti informatici e trattamento illecito dei dati, introdotti dall'articolo 7 della Legge 18 marzo 2008, n. 48, che ha inserito nel D.Lgs. n. 231/01 l'articolo 24-*bis*;
iii) Delitti di Criminalità Organizzata, introdotti dall'articolo 2, comma 29, della Legge 15 luglio 2009, n. 94, che ha inserito nel D.Lgs. n. 231/01 l'articolo 24-*ter*;
iv) Reati in tema di falsità in monete, carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento, introdotti dall'articolo 6 della Legge 23 novembre 2001, n. 406, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*bis*, come modificato dall'articolo 15, comma 7, lett. a), della Legge 23 luglio 2009, n. 99;
v) Delitti contro l'industria e il commercio, introdotti dall'articolo 15, comma 7, lett. b), della Legge 23 luglio 2009, n. 99, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*bis*.1;
vi) Reati Societari, introdotti dal Decreto Legislativo 11 aprile 2002, n. 61, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*ter* anche come emendati dalla legge 190/12;
vii) Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, introdotti dalla Legge 14 gennaio 2003, n. 7, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*quater*;
viii) Delitti di pratiche di mutilazione degli organi genitali femminili, introdotti dalla Legge 9 gennaio 2006, n. 7, che ha inserito nel D.Lgs. n. 231/01 l'art. 25-*quater*.1;
ix) Delitti contro la Personalità Individuale, introdotti dalla Legge 11 agosto 2003, n. 228, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-quinquies, emendato ai sensi del D.Lgs. n.39 del 4 marzo 2014;
x) Reati di abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla Legge 18 aprile 2005, n. 62, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*sexies*;
xi) Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e sicurezza dei Lavoratori, introdotti dalla Legge 3 agosto 2007, n. 123, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*septies*;
xii) Reati di Ricettazione, Riciclaggio e Impiego di denaro, beni o utilità di provenienza illecita, nonché Autoriciclaggio, introdotti dal Decreto Legislativo 21 novembre 2007, n. 231, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*octies* (il reato di Autoriciclaggio, invece, è stato inserito con la Legge 186/2014);
xiii) Delitti in materia di Violazione del Diritto d'Autore, introdotti dall'articolo 15, comma 7, lett. c), della Legge 23 luglio 2009, n. 99, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*novies*;
xiv) Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dall'art. 4 della Legge 3 agosto 2009, n. 116, che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*decies*;

xv) Reati Ambientali, introdotti dall'art. 2 del D.Lgs. n. 121 del 7 luglio 2011, che ha inserito nel D.Lgs. 231/01 l'articolo 25-*undecies.*

xvi) Delitto di impiego di cittadini di Paesi terzi di cui il soggiorno è irregolare, introdotto dal Decreto Legislativo 16 luglio 2012, n. 109, recante l'"Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare", che ha inserito nel D.Lgs. n. 231/01 l'articolo 25-*duodecies;*

xvii) Reati transnazionali, introdotti dalla Legge 16 marzo 2006, n.146 "Legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale".

1.4. Le sanzioni previste nel Decreto a carico dell'ente

Le sanzioni previste dal D.Lgs. n. 231/01 per gli illeciti amministrativi dipendenti da reato sono le seguenti:

- ***sanzioni amministrative pecuniarie;***
- ***sanzioni interdittive;***
- ***confisca;***
- ***pubblicazione della sentenza.***

La sanzione ***amministrativa pecuniaria***, disciplinata dagli articoli 10 e seguenti del Decreto, costituisce la sanzione "di base" di necessaria applicazione, del cui pagamento risponde l'ente con il suo patrimonio o con il fondo comune.

Il Legislatore ha adottato un criterio innovativo di commisurazione della sanzione, attribuendo al Giudice l'obbligo di procedere a due diverse e successive operazioni di apprezzamento. Ciò comporta un maggiore adeguamento della sanzione alla gravità del fatto ed alle condizioni economiche dell'ente.

La prima valutazione richiede al Giudice di determinare il numero delle quote (in ogni caso non inferiore a cento, né superiore a mille) tenendo conto:

- della gravità del fatto;
- del grado di responsabilità dell'ente;
- dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Nel corso della seconda valutazione il Giudice determina, entro i valori minimi e massimi predeterminati in relazione agli illeciti sanzionati, il valore di ciascuna quota, da un minimo di Euro 258,00 ad un massimo di Euro 1.549,00. Tale importo è fissato "*sulla base delle condizioni economiche e patrimoniali dell'ente, allo scopo di assicurare l'efficacia della sanzione*" (articoli 10 e 11, comma 2°, D.Lgs. n. 231/01).

Come affermato al punto 5.1. della Relazione al Decreto, *"Quanto alle modalità di accertamento delle condizioni economiche e patrimoniali dell'ente, il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazione le dimensioni dell'ente e la sua posizione sul mercato. (...). Il giudice non potrà fare a meno di calarsi, con l'ausilio di consulenti, nella realtà dell'impresa, dove potrà attingere anche le informazioni relative allo stato di solidità economica, finanziaria e patrimoniale dell'ente".*

L'articolo 12, D.Lgs. n. 231/01, prevede una serie di casi in cui la sanzione pecuniaria viene ridotta. Essi sono schematicamente riassunti nella seguente tabella, con indicazione della riduzione apportata e dei presupposti per l'applicazione della riduzione stessa.

Riduzione	***Presupposti***
1/2 (e non può comunque essere superiore ad Euro 103.291,00)	• L'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi *e* l'Ente non ne ha ricavato un vantaggio o ne ha ricavato un vantaggio minimo; *ovvero* • Il danno patrimoniale cagionato è di particolare tenuità.
da 1/3 a 1/2	[Prima della dichiarazione di apertura del dibattimento di primo grado] • L'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *ovvero* • È stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.
da 1/2 a 2/3	[Prima della dichiarazione di apertura del dibattimento di primo grado] • L'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; • È stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Le ***sanzioni interdittive*** previste dal Decreto sono quelle di seguito riportate e si applicano solo in relazione ai reati per i quali sono espressamente previste all'interno di tale testo normativo:

- interdizione dall'esercizio dell'attività aziendale;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Perché possano essere comminate, occorre inoltre che ricorra almeno una delle condizioni di cui all'articolo 13, D.Lgs. n. 231/01, ossia:

- ✓ "*l'ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative*"; ovvero
- ✓ "*in caso di reiterazione degli illeciti*"[3].

[3] Ai sensi dell'articolo 20 del D.Lgs. n. 231/01, "*si ha reiterazione quanto l'ente, già condannato in via definitiva almeno una volta per un illecito dipendente da reato, ne commette un altro nei cinque anni successivi alla condanna definitiva*".

In ogni caso, non si procede all'applicazione delle *sanzioni interdittive*, quando il reato è stato commesso nel prevalente interesse dell'autore o di terzi e l'ente ne ha ricavato un vantaggio minimo o nullo, ovvero il danno patrimoniale cagionato è di particolare tenuità.

L'applicazione delle sanzioni interdittive è altresì esclusa dal fatto che l'ente abbia posto in essere le condotte riparatorie previste dall'articolo 17, D.Lgs. n. 231/01 e, più precisamente, quando concorrono le seguenti condizioni:

- ✓ "*l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso*";
- ✓ "*l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi*";
- ✓ "*l'ente ha messo a disposizione il profitto conseguito ai fini della confisca*".

Le sanzioni ***interdittive*** hanno una durata non inferiore a tre mesi e non superiore a due anni e la scelta della misura da applicare e della sua durata viene effettuata dal Giudice, sulla base dei criteri in precedenza indicati per la commisurazione della sanzione pecuniaria, "*tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso*" (art. 14, D.Lgs. n. 231/01).

Il Legislatore si è, poi, preoccupato di precisare che l'interdizione dell'attività ha natura residuale rispetto alle altre sanzioni interdittive.

Ai sensi dell'articolo 19, D.Lgs. n. 231/01, è sempre disposta, con la sentenza di condanna, la ***confisca*** – anche per equivalenti – del ***prezzo*** (denaro o altra utilità economica data o promessa per indurre o determinare un altro soggetto a commettere il reato) o del ***profitto*** (utilità economica immediata ricavata) del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede.

La ***pubblicazione della sentenza di condanna*** in uno o più giornali, per estratto o per intero, può essere disposta dal Giudice, unitamente all'affissione nel comune dove l'ente ha la sede principale, quando è applicata una sanzione interdittiva. La pubblicazione è eseguita a cura della Cancelleria del Giudice competente ed a spese dell'ente.

2 L'ADOZIONE DEL MODELLO

2.1. L'adozione del Modello di organizzazione e di gestione con finalità di esimente della responsabilità amministrativa

L'articolo 6 del D.Lgs. n. 231/2001 prevede che, se il reato è stato commesso da uno dei soggetti indicati dal Decreto, l'ente non risponda qualora provi che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e sull'osservanza dei modelli e di curarne l'aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
c) le persone hanno commesso il fatto eludendo fraudolentemente i modelli di organizzazione e di gestione;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)[4].

L'articolo 7 del D.Lgs. n. 231/01 stabilisce, inoltre, che, qualora il reato sia commesso da Soggetti Sottoposti alla vigilanza di un Soggetto Apicale, la responsabilità dell'ente sussiste se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Tuttavia, l'inosservanza di tali obblighi è esclusa, e con essa la responsabilità dell'ente, se prima della commissione del reato l'ente medesimo ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Si precisa altresì che, nell'ipotesi delineata dall'art. 6, (fatto commesso da Soggetti Apicali) l'onere di provare la sussistenza della situazione esimente grava sull'Ente, mentre nel caso configurato dall'art. 7 (fatto commesso da Soggetti Sottoposti all'altrui vigilanza), l'onere della prova in ordine all'inosservanza, ovvero all'inesistenza dei modelli o alla loro inidoneità grava sull'accusa.

La mera adozione del Modello da parte dell'organo dirigente – che è da individuarsi nell'organo titolare del potere gestorio – Consiglio di Amministrazione – non pare tuttavia misura sufficiente a determinare l'esonero da responsabilità dell'ente, essendo piuttosto necessario che il Modello sia *efficace* ed *effettivo*.

Quanto all'efficacia del Modello, il Legislatore, all'art. 6 comma 2 D.Lgs. n. 231/2001, statuisce che il Modello deve soddisfare le seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati (cosiddetta "mappatura" delle attività a rischio);
b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

[4] La legge 12 novembre 2011, n. 183 recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato", nota anche come Legge di stabilità 2012, ha inserito all'art. 6 del Decreto Legislativo n. 231 il comma 4-bis, a norma del quale *"Nelle società di capitali il collegio sindacale, il consiglio di sorveglianza e il comitato per il controllo della gestione possono svolgere le funzioni dell'organismo di vigilanza di cui al comma 1, lettera b)"*.

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

2.2. Le Fonti del Modello: Linee Guida di Confindustria

Su espressa indicazione del Legislatore delegato, i modelli possono essere adottati sulla base di codici di comportamento redatti da associazioni rappresentative di categoria che siano stati comunicati al Ministero della Giustizia il quale, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sull'idoneità dei modelli a prevenire i reati.

La predisposizione del presente Modello è ispirata alle Linee Guida approvate da Confindustria e successivamente aggiornate nel marzo 2014.

Il percorso indicato dalle Linee Guida per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

a) individuazione delle Aree a Rischio;
b) predisposizione di un sistema di controllo in grado di ridurre i rischi attraverso l'adozione di appositi protocolli. A supporto di ciò soccorre l'insieme coordinato di strutture organizzative, attività e regole operative applicate – su indicazione del vertice apicale – dal *management* volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno.

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

- ✓ ***Codice Etico;***
- ✓ ***Sistema Organizzativo;***
- ✓ ***Procedure manuali ed informatiche;***
- ✓ ***Poteri autorizzativi e di firma;***
- ✓ ***Sistemi di controllo e gestione;***
- ✓ ***Comunicazioni al personale e sua formazione.***

Teleippica ha, quindi, provveduto alla rilevazione ed alla analisi dei presidi di controllo aziendali – il Codice Etico, il Sistema Organizzativo, il Sistema di attribuzione di poteri autorizzativi e di firma, il Sistema di Controllo, le iniziative di comunicazione al personale e di formazione, nonché le procedure esistenti e ritenute rilevanti ai fini della valutazione.

Premesso quindi che il Modello deve essere idoneo a prevenire i reati previsti dal Decreto, in una logica di gestione dei rischi "complessivi", Teleippica ha anche valorizzato la sinergia con il "*sistema di gestione di sicurezza delle informazioni*" ai sensi della dello standard UNI EN ISO 27001 per il quale Teleippica ha ottenuto la relativa certificazione.

Il sistema di controllo inoltre deve essere uniformato ai seguenti principi:

- verificabilità, tracciabilità, coerenza e congruenza di ogni operazione;

- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- introduzione di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal Modello.

2.3.Il Modello di Teleippica

Al fine di garantire condizioni di legalità, correttezza e trasparenza nello svolgimento della propria attività, Teleippica S.r.l. (di seguito "Teleippica" o "Società") ha ritenuto di provvedere alla definizione di un proprio Modello di Organizzazione, Gestione e Controllo (di seguito in breve anche "Modello") ai sensi del Decreto.

Il Modello, dunque, è indirizzato a tutti coloro i quali operano con la Società, che sono tenuti a conoscere e rispettare le disposizioni in esso contenute.

In particolare, i destinatari del Modello sono:

i. gli Organi Sociali (l'organo amministrativo, gli organi delegati, il collegio sindacale, nonché qualsiasi soggetto che eserciti, anche in via di fatto, i poteri di rappresentanza, decisionali e/o di controllo all'interno della Società) e la Società di Revisione;
ii. il Personale (ossia, i dipendenti, i lavoratori parasubordinati e i collaboratori coordinati e continuativi, ecc.) della Società;
iii. i Terzi: ossia: i consulenti, le controparti contrattuali, i fornitori, i clienti, i partner (laddove presenti), nonché tutti coloro che, pur esterni alla società, operino, direttamente o indirettamente, per Teleippica.

- ***Organi Sociali e il Personale***

  Tutti gli Amministratori, Sindaci e i Dipendenti, la Società di Revisione di Teleippica sono destinatari del Modello e devono attenersi alle disposizioni in esso contenute.

  In ordine alla determinazione della responsabilità dell'Ente, sono considerati Soggetti Apicali gli amministratori aziendali, i Sindaci, i dirigenti ed il personale che anche di fatto esercita attività direttive pur non essendo dirigente mentre sono considerati Soggetti Sottoposti all'altrui direzione i dipendenti non dirigenti dell'azienda.

- ***Soggetti Terzi***

  Si tratta, in particolare, di tutti i soggetti che non rivestono una posizione ''apicale'' nei termini specificati nei paragrafi precedenti e che sono comunque tenuti al rispetto del Modello in virtù della funzione svolta in relazione alla struttura societaria ed organizzativa della Società, ad esempio in quanto funzionalmente soggetti alla direzione o vigilanza di un soggetto "apicale", ovvero in quanto operanti, direttamente o indirettamente, per Teleippica.

  Nell'ambito di tale categoria, possono farsi rientrare:

  - tutti coloro che intrattengono con Teleippica un rapporto di lavoro di natura non subordinata (ad es., i collaboratori a progetto, i consulenti, i lavoratori somministrati);

- i collaboratori a qualsiasi titolo;
- tutti coloro che agiscono in nome e/o per conto della Società;
- i soggetti cui sono assegnati, o che comunque svolgono, funzioni e compiti specifici in materia di salute e sicurezza sul lavoro (ad es., i Medici Competenti e, qualora esterni all'azienda, i Responsabili e gli Addetti al Servizio Prevenzione e Protezione);
- i fornitori ed i partner.

Tra i Soggetti Terzi così definiti debbono ricondursi anche coloro che, sebbene abbiano un rapporto contrattuale con altra società del Gruppo, nella sostanza operano nell'ambito delle aree di attività sensibili per conto o nell'interesse di Teleippica.

Teleippica ritiene che l'adozione del Modello, unitamente all'emanazione di un Codice Etico, costituisca, al di là delle prescrizioni di legge, un ulteriore valido strumento di sensibilizzazione di tutti i dipendenti e di tutti coloro che a vario titolo collaborano con la Società, al fine di far seguire, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti in linea con i valori etico - sociali cui si ispira la Società nel perseguimento del proprio oggetto sociale, e tali comunque da prevenire il rischio di commissione dei reati contemplati dalla Legge.

In relazione ai Soggetti Terzi, Teleippica, tramite specifiche clausole contrattuali espresse, si impegna alla reale applicazione dei principi contenuti nel Modello, pena la risoluzione del rapporto (clausole risolutive espresse).

Teleippica, sensibile quindi all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, nonché consapevole dell'importanza di assicurare condizioni di correttezza nella conduzione degli affari e nelle attività aziendali a tutela della posizione e dell'immagine propria e delle aspettative dei soci cooperatori, adotta volontariamente il Modello di organizzazione gestione e controllo previsto dalla Legge, fissandone i principi di riferimento.

2.4. Approvazione, modifica, attuazione del Modello 231

Il Modello nella sua prima stesura è stato approvato, in conformità al disposto dell'art. 6, co. 1, lett. a) del Decreto, da Teleippica in data 03 novembre 2014.

Teleippica ha costituito l'Organismo di Vigilanza deputato a vigilare sul funzionamento e sull'osservanza del Modello in conformità a quanto previsto dal Decreto.

La Società anche a mezzo dell'Organismo di Vigilanza ha continuato a monitorare il Modello, disponendo un aggiornamento alla luce dell'evoluzione normativa.

Il presente aggiornamento, da considerarsi sostitutivo delle precedenti stesure del Modello, è stato adottato da Teleippica con delibera del Consiglio di Amministrazione.

L'aggiornamento ha riguardato l'integrazione della Parte Speciale F al fine di recepire il nuovo reato di Autoriciclaggio introdotto nel D.Lgs. 231/01 dalla Legge 186/2014 recante "*Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio*".

2.5.Metodologia - La costruzione del Modello

Teleippica ha effettuato la mappatura delle aree a rischio ai sensi del Decreto, mediante l'identificazione e valutazione dei rischi relativi alle fattispecie di reato oggetto della normativa e del relativo sistema di controllo interno, nonché la definizione della prima stesura del Modello, sulla base delle attività di cui ai punti precedenti.

La redazione del Modello è stata articolata nelle fasi di seguito descritte:

a) esame preliminare del contesto aziendale attraverso lo svolgimento di incontri con i principali responsabili al fine di effettuare una prima analisi dell'organizzazione e delle attività svolte dalle varie funzioni organizzative, nonché di identificare i processi aziendali nei quali tali attività sono articolate e la loro concreta ed effettiva attuazione;

b) individuazione delle aree di attività e dei processi aziendali a "rischio" alla commissione dei reati, operata sulla base dell'esame preliminare del contesto aziendale di cui alla precedente lettera a) nonché individuazione delle possibili modalità di commissione dei reati;

c) analisi, tramite incontri con i responsabili delle "Aree a Rischio Reato" identificate, dei principali fattori di rischio connessi ai reati di cui al Decreto, nonché rilevazione, analisi e valutazione dell'adeguatezza dei controlli aziendali esistenti;

d) identificazione dei punti di miglioramento del sistema di controllo interno e definizione di uno specifico piano di attuazione dei punti di miglioramento individuati.

Al termine delle suddette attività, è stato messo a punto un elenco delle Aree a Rischio Reato, ovvero di quei settori della Società e/o processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente, alla luce delle attività svolte, il rischio di commissione dei reati, tra quelli indicati dal Decreto, ed astrattamente riconducibili alla tipologia di attività svolta dalla Società.

Teleippica ha, quindi, provveduto alla rilevazione ed alla analisi dei controlli aziendali - verificando il Sistema Organizzativo, il Sistema di attribuzione di Procure e Deleghe, il Sistema di Controllo di Gestione, nonché le procedure esistenti e ritenute rilevanti ai fini dell'analisi (c.d. fase as is analysis) – nonché alla successiva identificazione dei punti di miglioramento, con la formulazione di appositi suggerimenti, nonché dei piani di azione per l'implementazione dei principi di controllo (c.d. gap analysis).

Sono state altresì individuate le aree nel cui ambito sono gestiti strumenti di tipo finanziario e/o mezzi sostitutivi che possono supportare la commissione dei reati nelle aree a rischio reato.

Unitamente all'attività di *risk assessment* e di identificazione dei punti di controllo esistenti, Teleippica ha effettuato un'attenta ricognizione delle rimanenti componenti fondamentali del Modello, ovvero:

- il Codice Etico;
- il Sistema Disciplinare;
- la disciplina dell'OdV;
- i flussi dell'OdV.

2.6. Teleippica Srl e la sua mission

Teleippica è una Società del Gruppo SNAI, con sedi a Porcari (Lu) e a Roma (RM), che sulla base di apposite autorizzazioni pubbliche (concessioni radio-televisive), cura la diffusione delle immagini televisive e multimediali legate al mondo dell'ippica e di tutti gli aspetti di costume collegati a tale sport (es. scommesse sulle corse, attività ippica nazionale e internazionale, allevamento e promozione dei cavalli, ecc.).

Teleippica cura anche la gestione di un canale radio "Radio Snai" appositamente dedicato a servizi aventi ad oggetto manifestazioni sportive e di promozione dell'ippica nazionale ed internazionale.

2.7. Le categorie di reato rilevanti per Teleippica Srl

Alla luce dell'analisi svolta dalla Società ai fini della predisposizione del presente Modello, le categorie di reato previste dal D.Lgs. 231/01, che potenzialmente potrebbero comportare la responsabilità amministrativa della Società, sono quelle di seguito riportate:

- Reati contro la P.A. (artt. 24 e 25);
- Reati societari (art. 25 *ter*, così come modificato dalla L. 190/2012 che ha, tra l'altro, introdotto il reato di corruzione tra privati);
- 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 (art. 25 *septies*);
- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 *octies*);
- Delitti informatici e trattamento illecito dei dati (art. 24 *bis*);
- Delitti di criminalità organizzata (art. 24 *ter*);
- Delitti in materia di violazione del diritto d'autore (art. 25-*novies*);
- Reato di Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies*);
- Reati Ambientali (art. 25-*undecies*);
- Delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25- *duodecies*).

Per quanto riguarda le restanti categorie di reato si è ritenuto che, alla luce della attività principale svolta dalla Società, del contesto socio-economico in cui opera e dei rapporti e delle relazioni giuridiche ed economiche che la stessa instaura con soggetti terzi, non siano presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della Società stessa.

Al riguardo, si è comunque provveduto a presidiare tali rischi attraverso i principi di comportamento sanciti nel Codice Etico di Teleippica che vincolano in ogni caso i Destinatari al rispetto dei valori essenziali quali imparzialità, correttezza, trasparenza, rispetto per la persona umana, correttezza e legalità.

La Società si impegna a valutare costantemente la rilevanza, ai fini del presente Modello, di eventuali ulteriori reati, attualmente previsti dal D. Lgs 231/01 o introdotti da successive integrazioni allo stesso.

Per ciascuna delle categorie di reato considerate rilevanti per Teleippica (ad eccezione che per gli artt. 24 *ter*, 25-*octies*, 25-*undecies* e 25-*duodecies*) sono state individuate, nella relativa Parte Speciale, le c.d. "attività a rischio", ossia quelle attività nello svolgimento delle quali è astrattamente possibile che sia commesso un reato, le relative modalità di commissione ed i controlli aziendali esistenti.

Per quanto concerne i reati di cui agli artt. 24 *ter*, 25-*octies*, 25-*undecies* e 25-*duodecies*, l'esito dell'attività di *risk assessment* ha portato a ritenere, sebbene applicabili e rilevanti, minore la concreta possibilità di commissione di tali reati, in virtù dell'attività svolta dalla Società. Pertanto in relazione a tali tipologie di reato trovano applicazione i principi di controllo descritti nella Parte Speciale F e nel Codice Etico.

2.8. La finalità e la struttura del modello organizzativo

Il presente Documento tiene conto della particolare realtà imprenditoriale di Teleippica e rappresenta un valido strumento di sensibilizzazione ed informazione dei Soggetti Apicali, dei Soggetti Sottoposti e dei Terzi. Tutto ciò, affinché i Destinatari seguano, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti, in linea con i valori etico-sociali cui si ispira la Società nel perseguimento del proprio oggetto sociale e tali comunque da prevenire il rischio di commissione dei reati previsti dal Decreto.

Il Modello si compone della presente Parte Generale e le seguenti Parti Speciali, nonché gli ulteriori documenti dallo stesso richiamati e/o di seguito elencati:

- Parte Speciale A:
  - ✓ Sezione 1: descrizione dei Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia;
  - ✓ Sezione 2: Aree a Rischio relative ai Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, relative modalità di commissione e Controlli Aziendali esistenti al fine della prevenzione dei reati *de quo*;

- Parte Speciale B:
  - ✓ Sezione 1: descrizione dei Reati societari;
  - ✓ Sezione 2: Aree a Rischio relative ai Reati societari, relative modalità di commissione e Controlli Aziendali esistenti al fine della prevenzione dei reati *de quo*;

- Parte Speciale B1:
  - ✓ Sezione 1: descrizione del Reato di Corruzione tra privati;
  - ✓ Sezione 2: Aree a Rischio relative al delitto di Corruzione tra privati, relative modalità di commissione e Controlli Aziendali esistenti al fine della prevenzione dei reati *de quo*;

- Parte Speciale C:
  - ✓ Sezione 1: descrizione dei 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;

  - ✓ Sezione 2: Aree a Rischio relative 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, relative modalità di commissione e Controlli Aziendali esistenti al fine della prevenzione dei reati *de quo*;

- Parte Speciale D:
  - ✓ Sezione 1: descrizione dei Delitti informatici e trattamento illecito dei dati;
  - ✓ Sezione 2: Aree a Rischio relative ai Delitti informatici e trattamento illecito dei dati, relative modalità di commissione e Controlli Aziendali esistenti al fine della prevenzione dei reati *de quo*;

- Parte Speciale E:
  - ✓ Sezione 1: descrizione dei Delitti in materia di violazione del Diritto d'Autore;
  - ✓ Sezione 2: Aree a Rischio relative ai Delitti in materia di violazione del Diritto d'Autore, relative modalità di commissione e Controlli Aziendali esistenti al fine della prevenzione dei reati *de quo*;

- Parte Speciale F: contenente i Principi generali di condotta applicabili alle famiglie di reato di cui agli artt. (i) 24-ter; (ii) 25-octies; (iii) 25-undecies (iv) 25-duodecies.

Fermo restando quanto previsto nelle Parti Speciali da A ad F al presente Documento, Teleippica ha definito uno specifico sistema di deleghe e procure, procedure, protocolli e controlli interni aventi quale finalità quella di garantire un'adeguata trasparenza e conoscibilità dei processi decisionali e finanziari, nonché dei comportamenti che devono essere tenuti dai Soggetti Apicali e dai Soggetti Sottoposti, operanti nelle aree aziendali.
Si precisa, inoltre che costituiscono parte integrante e sostanziale del presente Modello, i seguenti documenti:

- il Codice Etico della Società, nel quale sono definiti i principi fondamentali a cui Teleippica si ispira ed intende uniformare la propria attività;
- il Sistema Disciplinare e relativo meccanismo sanzionatorio, da applicare in caso di violazione del Modello.

Il Modello si propone come finalità quella di:

- rendere tutti i Destinatari che operano in nome e per conto di Teleippica, ed in particolare quelli impegnati nelle Aree a Rischio, consapevoli di poter incorrere, in caso di violazione delle disposizioni in esso riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti, ma anche nei confronti della Società;
- informare tutti i Destinatari che operano con la Società che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale;
- confermare che la Società non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità e che, in ogni caso, tali comportamenti (anche nel caso in cui la Società fosse

apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi cui è ispirata l'attività imprenditoriale di Teleippica.

2.9. Il concetto di rischio accettabile

Nella predisposizione del Modello, non può essere trascurato il concetto di rischio "accettabile".

E' importante che ai fini dell'applicazione delle norme del Decreto sia definita una soglia effettiva che consenta di porre un limite alla quantità/qualità delle misure di prevenzione da introdurre per evitare la commissione dei reati considerati.

In assenza di una previa determinazione del rischio "accettabile", la quantità/qualità di controlli preventivi istituibili è, infatti, virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale.

Riguardo al sistema di controllo preventivo da costruire in relazione al rischio di commissione delle fattispecie di reato contemplate dal Decreto, la soglia concettuale di accettabilità è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente.

Questa soluzione è in linea con la logica della "elusione fraudolenta" del Modello quale esimente ai fini dell'esclusione della responsabilità amministrativa dell'ente (art. 6, comma 1, lett. c, "*le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione*"), come chiarito dal più recente aggiornamento delle linee guida Confindustria.

Con specifico riferimento al meccanismo sanzionatorio introdotto dal Decreto, la soglia di accettabilità è pertanto rappresentata dall'efficace implementazione di un adeguato sistema preventivo che sia tale da non poter essere aggirato se non intenzionalmente, ovvero, ai fini dell'esclusione della responsabilità amministrativa dell'ente, le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il Modello ed i controlli adottati dalla Società.

2.10. Gestione delle risorse finanziarie

Tenuto conto che ai sensi dell'articolo 6, lettera c) del D.Lgs. n. 231/01 tra le esigenze cui il Modello deve rispondere vi è anche l'individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati, la Società ha adottato degli specifici protocolli e/o procedure contenenti i principi ed i comportamenti da seguire nell'ambito della gestione di tali risorse.

2.11. Processi esternalizzati

Alcuni dei processi aziendali a "rischio" identificati all'interno delle Parti Speciali del presente Modello, o porzioni di essi, sono stati esternalizzati ad altre società, anche facenti parte del Gruppo SNAI.

Con l'obiettivo di prevenire la commissione di reati presupposto nell'ambito dei processi esternalizzati, la Società ha definito la politica per la esternalizzazione delle proprie attività, individuando:

- le attività esternalizzate;
- i metodi per la valutazione del livello delle prestazioni del fornitore (*service level agreement,* di seguito in breve anche "S.L.A.").

Nel rispetto di tali criteri, la Società ha stipulato contratti di *outsourcing* per la regolamentazione dei rapporti con altre società, anche facenti parte del Gruppo SNAI, che forniscono servizi in favore della stessa.

Detti contratti prevedono:

- in maniera chiara l'attività oggetto della cessione, le modalità di esecuzione e il relativo corrispettivo;
- che il fornitore dà adeguata esecuzione alle attività esternalizzate nel rispetto della normativa vigente e delle disposizioni della Società;
- che il fornitore informa tempestivamente la Società di qualsiasi fatto che possa incidere in maniera rilevante sulla propria capacità di eseguire le attività esternalizzate in conformità alla normativa vigente e in maniera efficiente ed efficace;
- che il fornitore garantisce la riservatezza dei dati relativi alla Società e ai suoi clienti;
- che la Società ha facoltà di controllo e accesso all'attività e alla documentazione del fornitore;
- che il fornitore garantisce l'accesso completo ed immediato delle autorità competenti, in caso di richiesta, ai locali e alla documentazione del fornitore stesso;
- che la Società può recedere dal contratto senza oneri sproporzionati o tali da pregiudicare, in concreto, l'esercizio del diritto di recesso;
- che il contratto non può essere oggetto di sub-cessione senza il consenso della Società.

In materia di responsabilità amministrativa degli enti ed al fine di definire il perimetro della responsabilità stessa, è, inoltre, previsto che attraverso detti contratti le parti si danno reciprocamente atto di avere ciascuna adottato un Modello di organizzazione e gestione ai sensi del Decreto e successive integrazioni e modificazioni, e di monitorare ed aggiornare con regolarità il proprio rispettivo Modello, tenendo in considerazione i rilevanti sviluppi normativi ed organizzativi, ai fini della più ampia tutela delle rispettive società.

Le parti si impegnano nei confronti l'una dell'altra al rispetto più rigoroso dei propri Modelli, con particolare riguardo alle aree di detti Modelli che presentano rilevanza ai fini delle attività gestite mediante contratto di *outsourcing* e della sua esecuzione, e si impegnano altresì a darsi reciprocamente notizia di eventuali violazioni, che dovessero verificarsi e che possano avere attinenza con il contratto e/o la sua esecuzione. Più in generale, le parti si impegnano ad astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che, singolarmente o congiuntamente ad altre, possano integrare una qualsivoglia fattispecie di reato contemplata dal Decreto.

Con riferimento a tali rapporti contrattuali, Teleippica e le società che forniscono il servizio hanno rispettivamente e formalmente nominato i "Gestori del contratto". Essi sono responsabili della corretta esecuzione contrattuale e del relativo controllo tecnico-operativo ed economico dei servizi e delle forniture e rappresentano il riferimento, all'interno delle società e verso i terzi, dei contratti stipulati per i quali sono incaricati.
Il ruolo di "Gestore del contratto" viene individuato e formalizzato mediante apposito strumento organizzativo e comunicato tra le parti.

2.12. Corporate Governance

Consiglio di Amministrazione
La Società è amministrata da un Consiglio di Amministrazione composto attualmente da n. 5 membri nominati dall'Assemblea.
Il Consiglio provvede alla gestione dell'azienda assumendo tutte le decisioni ordinarie e straordinarie per il raggiungimento dell'oggetto sociale.

Assemblea dei Soci
L'Assemblea è convocata ai sensi dell'Art. 2484 C.C..

Sono tuttavia valide le assemblee anche senza formale convocazione se sia presente o vi sia validamente rappresentato l'intero Capitale Sociale e vi assista l'organo amministrativo e, se esistente, il Collegio Sindacale.
L'assemblea ordinaria deve essere convocata almeno una volta all'anno entro quattro mesi, o qualora particolari esigenze lo richiedano, entro sei mesi dalla chiusura dell'Esercizio Sociale.
L'assemblea può essere convocata presso la Sede Legale o altrove, purché nell'ambito del territorio nazionale.

Società di Revisione
L'Assemblea dei soci di Teleippica ha affidato ad una Società di Revisione, iscritta all'Albo Speciale, l'incarico di revisione e controllo contabile dei conti della Società.

2.13. Il sistema di controllo interno

Il sistema di controllo interno è l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati. Ogni persona che fa parte dell'organizzazione di Teleippica è parte integrante del suo sistema di controllo interno ed ha il dovere di contribuire, nell'ambito delle funzioni ed attività svolte, al suo corretto funzionamento.

Il ***Collegio Sindacale*** ha il compito di verificare:

- ✓ *l'osservanza della Legge e dell'Atto Costitutivo;*
- ✓ *il rispetto dei principi di corretta amministrazione;*
- ✓ *l'adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del sistema amministrativo contabile, anche in riferimento all'affidabilità di quest'ultimo a rappresentare correttamente i fatti di gestione.*

Il Collegio Sindacale di Teleippica si compone di 4 membri effettivi e 1 supplente.

Controlli interni e esterni al sistema

Tali controlli si ispirano ai seguenti principi:

- ✓ ***Separazione dei compiti.*** L'assegnazione dei compiti e dei conseguenti livelli autorizzativi deve essere volta a tenere distinte le funzioni di autorizzazione, esecuzione e controllo e comunque ad evitare la concentrazione in capo ad un unico soggetto;
- ✓ ***Formalizzazione dei poteri di firma e autorizzativi.*** Il conferimento di tali poteri deve essere coerente e commisurato ai compiti assegnati e formalizzato mediante un sistema di deleghe e procure che identifichi l'ambito di esercizio e la conseguente assunzione di responsabilità;
- ✓ ***Conformità alle regole comportamentali contenute nel Codice etico.*** Tutte le procedure aziendali devono uniformarsi ai principi dettati dal Codice etico adottato da Teleippica;
- ✓ ***Formalizzazione del controllo.*** I processi aziendali sensibili debbono essere tracciabili (in via documentale o informatica, con netta preferenza per quest'ultima) e prevedono specifici controlli di linea;
- ✓ ***Codificazione dei processi.*** I processi aziendali sono disciplinati secondo procedure volte a definirne tempistiche e modalità di svolgimento, nonché criteri oggettivi che governano i processi decisionali e gli indicatori di anomalia.

3 L'ORGANISMO DI VIGILANZA

3.1. Le caratteristiche dell'Organismo di Vigilanza

Secondo le disposizioni del D.Lgs. n. 231/01 (artt. 6 e 7), le indicazioni contenute nella Relazione al D.Lgs. n. 231/01 e gli orientamenti dottrinali e giurisprudenziali formatisi sul punto, le caratteristiche dell'Organismo di Vigilanza, tali da assicurare un'effettiva ed efficace attuazione del Modello, debbono essere:

a) autonomia ed indipendenza;
b) professionalità;
c) continuità d'azione;
d) onorabilità.

a) Autonomia ed indipendenza:

I requisiti di autonomia ed indipendenza sono fondamentali affinché l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo e, dunque, non subisca condizionamenti o interferenze da parte dell'organo dirigente.

Tali requisiti si possono ottenere garantendo all'OdV la posizione gerarchica più elevata possibile, e prevedendo un'attività di *reporting* al massimo vertice operativo aziendale, ovvero al Consiglio di Amministrazione nel suo complesso. Ai fini dell'indipendenza è inoltre indispensabile che all'OdV non siano attribuiti compiti operativi, che ne comprometterebbero l'obiettività di giudizio con riferimento alle verifiche sui comportamenti e sull'effettività del Modello. A tal fine è dotato di un apposito budget di spesa.

b) Professionalità:

L'OdV deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, ne garantiscono l'obiettività di giudizio[5].

c) Continuità d'azione:

L'OdV deve:

- svolgere in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine;
- essere una struttura riferibile alla Società, in modo da garantire la dovuta continuità nell'attività di vigilanza.

[5] Ci si riferisce, tra l'altro, a: tecniche di analisi e valutazione dei rischi; misure per il loro contenimento (procedure organizzative,, meccanismi di contrapposizione dei compiti, ecc.); *flow charting* di procedure e processi per l'individuazione dei punti di debolezza, tecniche di intervista e di elaborazione dei questionari; metodologie per l'individuazione di frodi; ecc. L'Organismo di Vigilanza deve avere competenze di tipo ispettivo (per accertare come si sia potuto verificare un reato della specie in esame e di chi lo abbia commesso); competenze di tipo consulenziale (per adottare – all'atto del disegno del Modello e delle successive modifiche – le misure più idonee a prevenire, con ragionevole certezza, la commissione dei reati medesimi) o, ancora, correntemente per verificare che i comportamenti quotidiani rispettino effettivamente quelli codificati) e competenze giuridiche.

d) Onorabilità:

I membri dell'OdV devono essere in possesso dei seguenti requisiti:

- non trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- non trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 c.c., con riferimento agli amministratori e da ritenersi applicabile, ai fini del Modello, anche ai singoli componenti dell'OdV;
- non essere stati sottoposti a misure di prevenzione ai sensi della Legge 27 dicembre 1956, n. 1423 ("Misure di prevenzione nei confronti delle persone pericolose per la sicurezza e la pubblica moralità") o della Legge 31 maggio 1965, n. 575 ("Disposizioni contro la mafia") e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- non aver riportato condanna, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
  - ✓ per uno dei delitti previsti dal R.D. 16 marzo 1942, n. 267 (Legge Fallimentare);
  - ✓ per uno dei delitti previsti dal Titolo XI del Libro V del Codice Civile ("Disposizioni penali in materia di società e consorzi");
  - ✓ per un delitto non colposo, per un tempo non inferiore a un anno;
  - ✓ per un delitto contro la Pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica.

Ciascun componente dell'OdV sottoscrive apposita dichiarazione attestante la sussistenza dei requisiti personali richiesti.

In caso di venir meno dei requisiti previsti, il componente dell'OdV decade, secondo quanto previsto al successivo paragrafo 3.4.

3.2. L'individuazione dell'Organismo di Vigilanza

In ossequio alle prescrizioni del D.Lgs. 231/2001, alle indicazioni espresse dalle Linee Guida di Confindustria e agli orientamenti della giurisprudenza formatisi in materia, Teleippica ha ritenuto di istituire un organo collegiale che, per la composizione scelta, possa assicurare la conoscenza delle attività aziendali, competenze in auditing, in campo legale e - al contempo - abbia autorevolezza e indipendenza tali da poter garantire la credibilità delle relative funzioni.

3.3. La durata dell'incarico e le cause di cessazione

L'OdV resta in carica per la durata indicata nell'atto di nomina e può essere rinnovato.

La cessazione dall'incarico dell'OdV può avvenire per una delle seguenti cause:

- ✓ scadenza dell'incarico;
- ✓ revoca dell'OdV da parte del Consiglio di Amministrazione;
- ✓ rinuncia del componente dell'OdV, formalizzata mediante apposita comunicazione scritta inviata al Consiglio di Amministrazione;

- ✓ verificarsi di una delle cause di decadenza di cui al successivo paragrafo 3.4.

La revoca dell'OdV può essere disposta solo per giusta causa e tali devono intendersi, a titolo esemplificativo, le seguenti ipotesi:

- il caso in cui il componente sia coinvolto in un processo penale avente ad oggetto la commissione di un reato ex D.Lgs. n. 231/01, dal quale possa derivare una responsabilità per la Società;
- il caso in cui sia riscontrata la violazione degli obblighi di riservatezza previsti a carico dell'OdV;
- una grave negligenza nell'espletamento dei compiti connessi all'incarico;
- il possibile coinvolgimento della Società in un procedimento, penale o civile, che sia connesso ad un'omessa o insufficiente vigilanza, anche colposa;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'OdV. In ogni caso, qualsiasi provvedimento di disposizione di carattere organizzativo che riguardi un membro dell'OdV (ad esempio, nel caso di cessazione rapporto di lavoro, spostamento ad altro incarico, licenziamento, provvedimenti disciplinari, nomina di nuovo responsabile) dovrà essere portato alla presa d'atto del Consiglio di Amministrazione per il tramite del Presidente dell'OdV;
- assenza ingiustificata a due o più riunioni consecutive dell'OdV, a seguito di rituale convocazione;
- essere stato condannato per uno dei reati contemplati nel D.Lgs. n. 231/01, anche se la sentenza non è passata in giudicato;
- l'impedimento del membro dell'OdV protratto per un periodo superiore a sei mesi, qualora si verifichino le cause di impedimento di cui al successivo paragrafo 3.5.

La revoca è disposta con delibera qualificata (due/ terzi) del Consiglio di Amministrazione previo parere non vincolante del Collegio Sindacale.

In caso di scadenza, revoca o rinuncia, il Consiglio di Amministrazione nomina senza indugio il nuovo componente dell'OdV, mentre il componente uscente rimane in carica fino alla sua sostituzione.

3.4. I casi di ineleggibilità e di decadenza

I membri dell'OdV sono scelti tra i soggetti qualificati ed esperti in ambito legale, di sistemi di controllo interno e/o tecnici specializzati.

Costituiscono motivi di ineleggibilità e/o di decadenza del componente dell'OdV:

a) la carenza o il venir meno dei requisiti di onorabilità di cui al precedente paragrafo 3.1;
b) l'esistenza di relazioni di parentela, coniugio o affinità entro il quarto grado con i membri del Consiglio di Amministrazione o del Collegio Sindacale della Società, o con i soggetti esterni incaricati della revisione;
c) con esclusivo riferimento ai componenti esterni dell'OdV, l'esistenza di rapporti di natura patrimoniale tra il componente e la Società, tali da compromettere l'indipendenza del componente stesso;
d) l'accertamento successivo alla nomina, che il membro dell'OdV abbia rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate,

con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la sua carica.

Qualora, nel corso dell'incarico, dovesse sopraggiungere una causa di decadenza, il componente dell'OdV è tenuto ad informare immediatamente il Consiglio di Amministrazione il quale nomina senza indugio il nuovo componente dell'OdV, mentre il componente uscente è tenuto ad astenersi dall'assumere qualsivoglia deliberazione, con la conseguenza che l'Organismo di Vigilanza opererà in composizione ridotta.

3.5. Cause di temporaneo impedimento

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea (per un periodo di tempo pari a sei mesi), ad un componente dell'OdV di svolgere le proprie funzioni o svolgerle con la necessaria autonomia ed indipendenza di giudizio, questi è tenuto a dichiarare la sussistenza del legittimo impedimento e - qualora esso sia dovuto ad un potenziale conflitto di interessi - la causa da cui il medesimo deriva, astenendosi dal partecipare alle sedute dell'organismo stesso o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso.

Nel caso di temporaneo impedimento o in ogni altra ipotesi che determini per uno o più componenti l'impossibilità di partecipare alla riunione, l'Organismo di Vigilanza opererà nella sua composizione ridotta.

3.6. Funzione, compiti e poteri dell'Organismo di Vigilanza

In conformità alle indicazioni fornite dal Decreto e dalle Linee Guida di Confindustria, la funzione del nominato OdV consiste, in generale, nel:

- vigilare sull'effettività del Modello, ossia vigilare affinché i comportamenti posti in essere all'interno dell'azienda corrispondano al Modello predisposto e che i destinatari dello stesso agiscano nella osservanza delle prescrizioni contenute nel Modello stesso;
- verificare l'efficacia e l'adeguatezza del Modello, ossia verificare che il Modello predisposto sia idoneo a prevenire il verificarsi dei reati di cui al Decreto;
- monitorare che il Modello sia costantemente aggiornato, proponendo al Consiglio di Amministrazione eventuali proposte di modifica dello stesso, al fine di adeguarlo ai mutamenti organizzativi, nonché alle modifiche normative e della struttura aziendale.

Nell'ambito della funzione sopra descritta, spettano all'OdV i seguenti compiti:

- verificare periodicamente l'adeguatezza dei Controlli Aziendali nell'ambito delle Aree a Rischio. A questo scopo, i Destinatari del Modello devono segnalare all'OdV le eventuali situazioni in grado di esporre la Società al rischio di reato. Tutte le comunicazioni devono essere redatte in forma scritta e trasmesse all'apposito indirizzo di posta elettronica attivato dall'OdV;
- effettuare periodicamente, sulla base del piano di attività dell'OdV previamente stabilito, verifiche ed ispezioni mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle Aree a Rischio;

- raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni di cui al successivo paragrafo 3.8) rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello, portate all'attenzione dell'OdV da specifiche segnalazioni o emerse nel corso dell'attività di vigilanza dello stesso;
- verificare che i Controlli Aziendali previsti nel Modello per le diverse tipologie di reato vengano effettivamente adottati ed implementati e siano rispondenti alle esigenze di osservanza del D.Lgs. n. 231/01, provvedendo, in caso contrario, a proporre azioni correttive ed aggiornamenti degli stessi;
- promuovere adeguate iniziative volte alla diffusione della conoscenza e della comprensione del Modello.

Per lo svolgimento delle funzioni e dei compiti sopra indicati, vengono attribuiti all'OdV i seguenti poteri:

- accedere in modo ampio e capillare ai vari documenti aziendali ed, in particolare, a quelli riguardanti i rapporti di natura contrattuale e non instaurati dalla Società con terzi;
- avvalersi del supporto e della cooperazione delle varie strutture aziendali e degli organi sociali che possano essere interessati, o comunque coinvolti, nelle attività di controllo;
- predisporre un piano annuale delle verifiche su adeguatezza e funzionamento del Modello;
- monitorare che la mappatura delle Aree a Rischio sia costantemente aggiornata, proponendo eventuali proposte di modifica della stessa, secondo le modalità e i principi seguiti nell'adozione del presente Modello;
- conferire specifici incarichi di consulenza ed assistenza a professionisti esperti in materia legale. A questo scopo, nella delibera del Consiglio di Amministrazione con cui viene nominato, all' OdV vengono attribuiti specifici poteri di spesa.

3.7.Obblighi di informazione nei confronti dell'Organismo di Vigilanza

L'articolo 6, II comma, lettera d) del Decreto, dispone che il Modello deve prevedere obblighi di informazione nei confronti dell'OdV, in modo che lo stesso possa espletare al meglio la propria attività di verifica. L'OdV, deve essere tempestivamente informato da tutti i soggetti aziendali, nonché dai terzi tenuti all'osservanza delle previsioni del Modello, di qualsiasi notizia relativa all'esistenza di possibili violazioni dello stesso.

L'OdV, deve essere tempestivamente informato da tutti i soggetti aziendali, nonché dai terzi tenuti all'osservanza delle previsioni del Modello, di qualsiasi notizia relativa all'esistenza di possibili violazioni dello stesso.

L'obbligo informativo è altresì rivolto a tutte le Funzioni aziendali e, in particolare, alle strutture ritenute a rischio di commissione di reati-presupposto di cui alla Mappatura delle Aree a Rischio Reato contenuta nel Modello.

In particolare, relativamente all'oggetto, i flussi informativi nei confronti dell'OdV possono essere classificati in:

1) ***Flussi informativi specifici periodici / occasionali che possono derivare dai soggetti aziendali presenti nelle aree a rischio;***
2) ***Segnalazioni.***

- **Flussi informativi specifici periodici / occasionali:**
  - ✓ I provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto che possano coinvolgere la Società, avviate anche nei confronti di ignoti;
  - ✓ Copia delle comunicazioni, richieste di informazioni o ordini di esibizione di documentazione a/da qualsiasi pubblica autorità direttamente o indirettamente ricollegabili a circostanze che possano far emergere responsabilità ai sensi del Decreto;
  - ✓ Le richieste di assistenza legale inoltrate dai dirigenti e dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
  - ✓ Eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili.
  - ✓ Gli aggiornamenti del sistema dei poteri e delle deleghe;
  - ✓ Le eventuali comunicazioni della società di revisione riguardanti possibili carenze nel sistema dei controlli interni;
  - ✓ I prospetti riepilogativi delle gare, pubbliche o a rilevanza pubblica, a livello nazionale/locale cui la Società ha partecipato per l'ottenimento delle concessioni pubbliche;
  - ✓ Le decisioni relative alla richiesta, erogazione e utilizzo di eventuali finanziamenti pubblici;
  - ✓ Bilancio annuale, corredato della nota integrativa, nonché la situazione patrimoniale semestrale;
  - ✓ Incarichi conferiti alla società di revisione;
  - ✓ Comunicazioni, da parte del Collegio Sindacale e della società di revisione, relative ad ogni criticità emersa, anche se risolta;
  - ✓ Ogni presunta o accertata violazione dei principi contenuti nel Modello, del Codice Etico e di Comportamento, delle procedure aziendali, e ogni altro aspetto potenzialmente rilevante ai fini dell'applicazione del Decreto;
  - ✓ Risultati di eventuali audit interni, condotti sulle Aree a Rischio Reato e segnalazione delle eventuali non conformità riscontrate;
  - ✓ Le relazioni dei procedimenti disciplinari attivati dalla Società in relazione alla violazione del Modello, del Codice Etico e di Comportamento, delle procedure aziendali e delle sanzioni applicate all'esito del procedimento, con la specifica delle ragioni che ne hanno legittimato l'irrogazione, nonché eventuali decisioni di archiviazione di un procedimento disciplinare o di non applicazione delle sanzioni con le relative motivazioni;
  - ✓ Eventuali emanazioni, modifiche ed integrazioni delle procedure operative e del sistema organizzativo aziendale della Società rilevanti ai fini del Modello;
  - ✓ Ogni segnalazione avente ad oggetto il funzionamento e l'aggiornamento del Modello e del Codice Etico e di Comportamento;
  - ✓ Le relazioni sulle attività di formazione aziendale pianificate;

- ✓ Eventuali comunicazioni della società di revisione riguardanti possibili carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società;
- ✓ La relazione periodica in merito alla casistica degli infortuni sul lavoro, dei mancati infortuni e delle malattie professionali per ciascun sito aziendale, con indicazione dei centri/reparti nei quali si sono verificati e delle cause che hanno cagionato tali infortuni;
- ✓ I verbali di sopralluogo delle autorità competenti che hanno evidenziato carenze organizzative con riferimento alla salute e sicurezza sul lavoro.

- ***Segnalazioni:***
  - ✓ Informazioni di ogni provenienza, anonime o meno, concernenti la possibile commissione di reati o comunque di violazioni del Modello applicato da Teleippica.

In ogni caso, i responsabili delle Funzioni interessate dalle attività a rischio comunicano all'OdV ogni informazione utile per agevolare lo svolgimento delle verifiche sulla corretta attuazione del Modello. In particolare, devono comunicare all'OdV, ogni anomalia o atipicità riscontrata nell'ambito delle attività svolte e informazioni disponibili.

Le segnalazioni all'OdV devono essere effettuate in forma scritta ed inviate all'indirizzo di posta elettronica appositamente istituito allo scopo odvteleippica@teleippica.it o anche in forma anonima ed inviate per iscritto all'Organismo.

L'OdV della Società agisce in modo da garantire i segnalanti contro qualsiasi tipo di ritorsione, intesa come atto che possa dar adito anche al solo sospetto di essere una forma di discriminazione o penalizzazione.

L'OdV garantirà adeguata riservatezza ai soggetti che riferiscono informazioni o compiono segnalazioni, fatti salvi gli obblighi di legge e la tutela dei diritti della Società.

3.8.Obblighi di informazione propri dell'Organismo di Vigilanza

Premesso che la responsabilità di adottare ed efficacemente implementare il Modello permane in capo al Consiglio di Amministrazione della Società, l'OdV riferisce in merito all'attuazione del Modello e al verificarsi di eventuali criticità.

L'OdV ha la responsabilità nei confronti del Consiglio di Amministrazione di:

- comunicare, all'inizio di ciascun esercizio e nell'ambito della propria relazione annuale, il piano delle attività che intende svolgere nell'anno stesso al fine di adempiere ai compiti assegnati. Tale piano sarà approvato dal Consiglio di Amministrazione stesso;
- relazionare, nell'ambito della propria relazione semestrale e annuale, lo stato di avanzamento del piano delle attività, unitamente alle eventuali modifiche apportate allo stesso, nonché in merito all'attuazione del Modello.

L'OdV, inoltre, comunica tempestivamente all'Amministratore Delegato eventuali problematiche connesse alle attività, laddove rilevanti.

L'OdV potrà relazionare periodicamente, oltre che il Consiglio di Amministrazione, anche il Collegio Sindacale in merito alle proprie attività.

L'OdV potrà richiedere di essere convocato dai suddetti organi per riferire in merito al funzionamento del Modello o a situazioni specifiche.
Gli incontri con gli organi sociali a cui l'OdV riferisce devono essere verbalizzati. Copia di tali verbali sarà custodita dall'OdV e dagli organi di volta in volta coinvolti.

L'OdV potrà, inoltre, a seconda delle singole circostanze:

- **A.** comunicare i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'OdV ottenga dai responsabili dei processi un piano delle azioni, con relativa tempistica, per l'implementazione delle attività suscettibili di miglioramento, nonché il risultato di tale implementazione;
- **B.** segnalare al Consiglio di Amministrazione e al Collegio Sindacale comportamenti/azioni non in linea con il Modello al fine di:
  - **i)** acquisire dal Consiglio di Amministrazione tutti gli elementi per effettuare eventuali comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
  - **ii)** dare indicazioni per la rimozione delle carenze, onde evitare il ripetersi dell'accadimento.

L'OdV ha l'obbligo di informare immediatamente il Collegio Sindacale, qualora la violazione riguardi il Consiglio di Amministrazione.

Infine, nell'ambito delle attività del Gruppo Snai, l'OdV della Società si coordina con gli altri OdV del Gruppo.

4 SISTEMA DISCIPLINARE

4.1. Principi generali

La Società prende atto e dichiara che la predisposizione di un adeguato sistema disciplinare e sanzionatorio per la violazione delle norme e disposizioni contenute nel Modello e nei relativi Controlli Aziendali è condizione essenziale per assicurare l'effettività del Modello stesso.

A questo proposito, infatti, gli articoli 6 comma 2, lettera e) e 7, comma 4, lettera b) del Decreto prevedono che i Modelli di organizzazione, gestione e controllo devono *"introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello"*, per i soggetti apicali e per i soggetti sottoposti.

Ai sensi dell'art. 2106 c.c., con riferimento ai rapporti di lavoro subordinato, il presente Sistema Sanzionatorio, integra, per quanto non espressamente previsto e limitatamente alle fattispecie ivi contemplate, i Contratti Collettivi Nazionali di Lavoro applicati al personale dipendente.

Il Sistema Sanzionatorio è suddiviso in sezioni, secondo la categoria di inquadramento dei destinatari ai sensi dell'art. 2095 c.c.

La violazione delle regole di comportamento e delle misure previste dal Modello, da parte di dipendenti della Società e/o di dirigenti della stessa, costituisce un inadempimento alle obbligazioni derivanti dal rapporto di lavoro, ai sensi dell'art. 2104 c.c. e dell'art. 2106 c.c.

L'applicazione delle sanzioni descritte nel Sistema Sanzionatorio prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello e dai relativi Controlli Aziendali sono assunti dalla Società in piena autonomia e indipendentemente dalla tipologia di illeciti di cui al Decreto.

Più precisamente, la mancata osservanza delle norme e delle disposizioni, contenute nel Modello e nei relativi Controlli Aziendali, lede, di per sé sola, il rapporto di fiducia in essere con la Società e comporta azioni di carattere sanzionatorio e disciplinare, a prescindere dall'eventuale instaurazione o dall'esito di un giudizio penale, nei casi in cui la violazione costituisca reato. Ciò anche nel rispetto dei principi di tempestività e immediatezza della contestazione (anche di natura disciplinare) e della irrogazione delle sanzioni, in ottemperanza alle norme di legge vigenti in materia.

Ai fini della valutazione dell'efficacia e dell'idoneità del Modello a prevenire i reati indicati dal D.Lgs. n. 231/2001, è necessario che il Modello individui e sanzioni i comportamenti che possono favorire la commissione di reati.

Il concetto di sistema disciplinare fa ritenere che la Società debba procedere ad una graduazione delle sanzioni applicabili, in relazione al differente grado di pericolosità che i comportamenti possono presentare rispetto alla commissione dei reati.

Ciò in quanto l'art. 6, comma, 2 D.Lgs. n. 231/2001, nell'elencare gli elementi che si devono rinvenire all'interno dei modelli predisposti dall'impresa, alla lettera e) espressamente prevede che l'impresa ha

l'onere di "*introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal modello*".

Il concetto di sistema disciplinare fa ritenere che la Società debba procedere ad una graduazione delle sanzioni applicabili, in relazione al differente grado di pericolosità che i comportamenti possono presentare rispetto alla commissione dei reati.

Si è pertanto creato un sistema disciplinare che, innanzitutto, sanzioni tutte le infrazioni al Modello, dalla più lieve alla più grave, mediante un sistema di *gradualità* della sanzione e che, secondariamente, rispetti il principio della *proporzionalità* tra la mancanza rilevata e la sanzione comminata.

A prescindere dalla natura del sistema disciplinare richiesto dal D.Lgs. n. 231/2001, resta la caratteristica di fondo del potere disciplinare che compete al Datore di Lavoro, riferito, ai sensi dell'art. 2106 c.c., a tutte le categorie di lavoratori ed esercitato indipendentemente da quanto previsto dalla contrattazione collettiva. In virtù dei principi esposti, il potere disciplinare di cui al D.Lgs. n. 231/2001 è esercitato dal Consiglio di Amministrazione a seguito di segnalazione e valutazione dello stesso.

4.2. Definizione di "Violazione" ai fini dell'operatività del presente Sistema Sanzionatorio

A titolo generale e meramente esemplificativo, costituisce "Violazione" del presente Modello e dei relativi Controlli Aziendali:

- ✓ la messa in atto di azioni o comportamenti, non conformi alla legge e alle prescrizioni contenute nel Modello stesso e nei relativi Controlli Aziendali, che comportino la commissione di uno dei reati contemplati dal Decreto;
- ✓ la messa in atto di azioni, l'omissione di azioni o comportamenti prescritti nel Modello e nei relativi Controlli Aziendali, che comportino una situazione di mero rischio di commissione di uno dei reati contemplati dal Decreto;
- ✓ l'omissione di azioni o comportamenti prescritti nel Modello e nei relativi Controlli Aziendali, che comporti un rischio di commissione di uno dei reati contemplati dal Decreto.

4.3. Criteri per l'irrogazione delle sanzioni

Il tipo e l'entità delle sanzioni specifiche saranno applicate in proporzione alla gravità della violazione e, comunque, in base ai seguenti criteri generali:

- elemento soggettivo della condotta (dolo, colpa);
- rilevanza degli obblighi violati;
- potenzialità del danno derivante alla Società e dell'eventuale applicazione delle sanzioni previste dal Decreto e da eventuali successive modifiche o integrazioni;
- livello di responsabilità gerarchica o tecnica del soggetto interessato;
- presenza di circostanze aggravanti o attenuanti, con particolare riguardo alle precedenti prestazioni lavorative svolte dal soggetto destinatario del Modello e ai precedenti disciplinari dell'ultimo biennio;
- eventuale condivisione di responsabilità con altri dipendenti o terzi in genere, che abbiano concorso nel determinare la violazione.

Qualora con un solo atto siano state commesse più infrazioni, punite con sanzioni diverse, si applicherà unicamente la sanzioni più grave.

I principi di tempestività ed immediatezza della contestazione, impongono l'irrogazione della sanzione (anche e soprattutto disciplinare) prescindendo dall'eventuale instaurazione e dall'esito di un giudizio penale.

In ogni caso le sanzioni disciplinari ai dipendenti dovranno essere irrogate nel rispetto dell'art. 7 della L. 300/70 (d'ora innanzi, per brevità, "Statuto dei lavoratori") e di tutte le altre disposizioni legislative e contrattuali esistenti in materia.

4.4. Le sanzioni

Lavoratori subordinati: illeciti disciplinari

Sono definiti illeciti disciplinari i comportamenti tenuti dai lavoratori dipendenti, ivi compresi i Dirigenti, in violazione delle regole e dei principi comportamentali previsti nel Modello. Il tipo e l'entità delle sanzioni applicabili ai singoli casi possono variare in relazione alla gravità delle mancanze e in base ai seguenti criteri:

- ✓ condotta (dolo o colpa) mansioni, qualifica e livello del dipendente;
- ✓ rilevanza degli obblighi violati;
- ✓ potenzialità del danno derivante a Teleippica;
- ✓ recidiva.

In caso di commissione di più violazioni, punibili con sanzioni diverse, potrà applicarsi la sanzione più grave. La violazione delle disposizioni potrà costituire inadempimento delle obbligazioni contrattuali, nel rispetto degli artt. 2104, 2106 e 2118 c.c., 7 della Legge 300/70, nonché della Legge 604/66, del CCNL applicato e vigente, con l'applicabilità, nei casi più gravi dell'art. 2119 c.c..

Criteri di correlazione

Al fine di esplicitare preventivamente i criteri di correlazione tra le mancanze dei lavoratori ed i provvedimenti disciplinari adottati, il Consiglio di Amministrazione classifica le azioni degli amministratori, dei dipendenti e degli altri soggetti terzi come segue:

- comportamenti tali da ravvisare una mancata esecuzione degli ordini impartiti da Teleippica sia in forma scritta che verbale nell'esecuzione di attività a rischio di reato, quali a titolo di esempio: violazione delle procedure, regolamenti, istruzioni interne scritte o verbali, violazione del codice etico che integrino gli estremi della colpa lieve (violazione di lieve entità);
- comportamenti tali da ravvisare una grave infrazione alla disciplina e/o alla diligenza nel lavoro quale l'adozione, nell'espletamento delle attività a rischio di reato, dei comportamenti di cui al punto 1) commessi con dolo o colpa grave (violazione di grave entità);
- comportamenti tali da provocare grave nocumento morale o materiale alla società, tali da non consentire la prosecuzione del rapporto neppure in via temporanea, quali l'adozione di comportamenti che integrino gli estremi di uno o più reati presupposto o comunque diretti in

modo non equivoco al compimento di tali reati (violazione di grave entità e con pregiudizio per Teleippica).

Nello specifico:

- mancato rispetto del Modello, qualora si tratti di violazioni realizzate nell'ambito delle attività "sensibili" di cui alle aree "strumentali" identificate nei documento di Sintesi del Modello (Parti Speciali A, B, B1, C, D, E, F);
- mancato rispetto del Modello, qualora si tratti di violazione idonea ad integrare il solo fatto (elemento oggettivo) di uno dei reati previsti nel Decreto;
- mancato rispetto del Modello, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto, o comunque sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto.

Trovano, inoltre, apposita evidenza le violazioni in materia di salute e sicurezza sul lavoro (Parte Speciale C), anch'esse ordinate secondo un ordine crescente di gravità:

- mancato rispetto del Modello, qualora la violazione determini una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione;
- mancato rispetto del Modello, qualora la violazione determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- mancato rispetto del Modello, qualora la violazione determini una lesione, qualificabile come "grave" ai sensi dell'art. 583, comma 1, cod. pen., all'integrità fisica di una o più persone, incluso l'autore della violazione;
- mancato rispetto del Modello, qualora la violazione determini una lesione, qualificabile come "gravissima" ai sensi dell'art. 583, comma 1, cod. pen., all'integrità fisica ovvero la morte di una o più persone, incluso l'autore della violazione.

Sanzioni applicabili a Quadri e Impiegati

A seguito del procedimento disciplinare ex art. 7, Legge 300/70, tenuto conto della gravità e/o reiterazione delle condotte, il lavoratore, responsabile di azioni od omissioni contrastanti con le prescrizioni del Modello, è soggetto alle seguenti sanzioni disciplinari:

- ✓ biasimo inflitto verbalmente (violazioni di lieve entità);
- ✓ biasimo inflitto per iscritto (violazioni di lieve entità);
- ✓ multa non eccedente le quattro ore di retribuzione (violazioni di grave entità);
- ✓ sospensione dalla retribuzione e dal servizio per un massimo di 8 giorni (violazioni di grave entità);
- ✓ licenziamento in tronco (violazioni di grave entità e con pregiudizio per Teleippica).

Sanzioni applicabili ai Dirigenti

Sebbene la procedura disciplinare ex art. 7, Legge 300/70 non sia applicabile ai Dirigenti, è opportuno prevedere la garanzia procedurale prevista dallo Statuto dei Lavoratori anche ai Dirigenti.
Tenuto conto della natura fiduciaria del rapporto di lavoro, in caso di violazioni delle disposizioni previste dal Modello, il Dirigente sarà soggetto alle seguenti sanzioni:

- ✓ lettera di richiamo (violazioni di lieve entità);

- ✓ risoluzione del rapporto (violazioni di grave entità e con pregiudizio per Teleippica).

Resta salvo il diritto al risarcimento per eventuali danni cagionati alla società da parte del Dirigente.

Procedura disciplinare per Amministratori e Sindaci

Nel caso di commissione di una Violazione di cui al precedente paragrafo 4.2. da parte di uno o più degli Amministratori della Società, l'OdV informa senza indugio il Consiglio di Amministrazione ed il Collegio Sindacale per le opportune valutazioni e provvedimenti.

Nell'ipotesi in cui sia stato disposto il rinvio a giudizio di uno o più degli Amministratori, presunti autori del reato da cui deriva la responsabilità amministrativa della Società, il Presidente del Consiglio di Amministrazione della Società convoca senza indugio l'Assemblea dei Soci per deliberare in merito alla revoca del mandato.

Nel caso di commissione di una Violazione di cui al precedente paragrafo 4.2. da parte di uno o più membri del Collegio Sindacale, l'OdV informa il Consiglio di Amministrazione e lo stesso Collegio Sindacale e il Presidente del Consiglio di Amministrazione convoca l'Assemblea dei Soci al fine di adottare gli opportuni provvedimenti.

Sanzioni applicabili a Terzi

La Società, in caso di violazione del Modello potrà:

- ✓ contestare l'inadempimento al destinatario, con la contestuale richiesta di adempimento degli obblighi contrattualmente assunti e previsti dal Modello, dalle procedure aziendali e dal Codice Etico, se del caso concedendo un termine ovvero immediatamente;
- ✓ richiedere un risarcimento del danno pari al corrispettivo percepito per l'attività svolta nel periodo decorrente dalla data dell'accertamento della violazione della raccomandazione all'effettivo adempimento.
- ✓ risolvere automaticamente il contratto in essere per grave inadempimento, ex artt. 1453 e 1455 c.c..

Tenuto conto della natura, del valore, della durata dell'incarico conferito da Teleippica Srl, si potrà valutare, caso per caso, l'opportunità di inserire clausole di risoluzione contrattuale, al fine di ottenere una funzione deterrente di condotte, anche solo sospette, di violazione e di predeterminare la quantificazione del danno, al quale potrà aggiungersi un ulteriore e maggiore danno da quantificarsi successivamente e in sede giudiziale.

Procedura disciplinare per il personale dipendente

La Società adotta una procedura aziendale standard per la contestazione degli addebiti disciplinari ai propri dipendenti e per l'irrogazione delle relative sanzioni, che rispetta le forme, le modalità e le tempistiche previste dall'art. 7 dello Statuto dei lavoratori, dal CCNL per i dipendenti di "Imprese Radio Televisive Private", nonché da tutte le altre disposizioni legislative e regolamentari in materia.

In seguito al verificarsi di una possibile Violazione del Presente Modello e delle relative Procedure, ai sensi del precedente punto 4.2 da parte di un dipendente, deve essere fatta tempestiva segnalazione dell'accaduto al Consiglio di Amministrazione, il quale valuta la gravità comportamento segnalato al fine di stabilire se sia necessario formulare una contestazione disciplinare nei confronti del dipendente interessato.

Nell'ipotesi in cui si valuti l'opportunità di irrogare una sanzione disciplinare più grave del rimprovero verbale, il Consiglio di Amministrazione contesta formalmente, mediante apposita Contestazione Disciplinare scritta, il comportamento disciplinarmente rilevante al dipendente interessato e lo invita a comunicare le proprie eventuali giustificazioni entro 5 giorni successivi la ricezione della Contestazione Disciplinare.

Laddove ricorra una possibile Violazione del Presente Modello e delle relative Procedure, ai sensi del precedente punto 4.2, da parte del dipendente interessato, la Contestazione Disciplinare scritta e le eventuali giustificazioni del medesimo devono essere trasmesse per conoscenza all'OdV.

L'OdV, laddove ravvisi una possibile Violazione del Presente Modello e dei relativi controlli, ai sensi del precedente punto 4.2, da parte del dipendente interessato, tenuto conto dei fatti contestati e delle eventuali giustificazioni presentate, può esprimere il proprio motivato parere in merito alla gravità dell'inadempimento e alle sanzioni da applicare.

Trascorsi almeno cinque giorni dalla consegna della Contestazione Disciplinare, il Consiglio di Amministrazione, tenuto conto del parere motivato, comunque non vincolante, dell'OdV, nonché delle eventuali giustificazioni del dipendente, decide se irrogare una sanzione in funzione della gravità della Violazione o dell'addebito contestato.

Laddove vi sia stata Violazione del Presente Modello e dei relativi Protocolli Organizzativi, ai sensi del precedente punto 4.2, da parte del dipendente interessato, il provvedimento disciplinare deve essere trasmesso per conoscenza all'OdV.

Il funzionamento e la corretta applicazione dei Protocolli di contestazione e sanzionamento degli illeciti disciplinari viene costantemente monitorato dal Consiglio di Amministrazione e dall'OdV.

4.5.Registro delle Violazioni

La Società predispone uno specifico registro delle Violazioni, contenente l'indicazione dei relativi responsabili, nonché delle sanzioni adottate nei loro confronti.

Il registro, tenuto a cura della funzione competente per le risorse umane di Teleippica, deve essere costantemente aggiornato e consultabile in qualsiasi momento dall'Organo di Amministrazione e dal Collegio Sindacale.

Nei rapporti con i Terzi, l'iscrizione in tale registro comporta il divieto di instaurazione di nuovi rapporti contrattuali con i soggetti interessati, salvo diversa decisione dell'Organo di Amministrazione.

5 AGGIORNAMENTO DEL MODELLO

L'adozione e l'efficace attuazione del Modello costituiscono per espressa previsione legislativa una responsabilità del Consiglio di Amministrazione.

Pertanto, il potere di aggiornare il Modello – espressione di un'efficace attuazione dello stesso – compete al Consiglio di Amministrazione, che lo esercita direttamente mediante delibera e con le modalità previste per l'adozione del Modello.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati indicati dal D.Lgs. n. 231/2001.

Compete all'Organismo di Vigilanza il compito di vigilare sull'aggiornamento del Modello, secondo quanto previsto nel presente Documento.

6 INFORMAZIONE E FORMAZIONE DEL PERSONALE

6.1. Diffusione del Modello

Le modalità di comunicazione del Modello devono essere tali da garantirne la piena pubblicità, al fine di assicurare che i Destinatari siano a conoscenza delle procedure e dei controlli che devono seguire per adempiere correttamente ai propri compiti o agli obblighi contrattuali instaurati con la Società.

Obiettivo di Teleippica è quello di comunicare i contenuti e i principi del Modello anche ai Soggetti Sottoposti ed ai soggetti Terzi, i quali si trovano ad operare – anche occasionalmente – per il conseguimento degli obiettivi della Società in forza di rapporti contrattuali.

A tal fine, il Modello è permanentemente archiviato nell'apposito "Archivio documentale", accessibile da parte di tutti i Soggetti Apicali e ai Soggetti Sottoposti. In tale "Archivio", inoltre, sono disponibili tutte le informazioni ritenute rilevanti per la conoscenza dei contenuti del Decreto e delle sue implicazioni per Teleippica.

Per quanto attiene ai Terzi, un estratto del presente Documento viene trasmesso agli stessi con espresso obbligo contrattuale di rispettarne le relative prescrizioni.

L'attività di comunicazione e formazione è supervisionata dall'OdV, avvalendosi delle strutture competenti, cui sono assegnati, tra gli altri, i compiti di promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, dei contenuti del D.Lgs. n. 231/2001, degli impatti della normativa sull'attività di Teleippica, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello e di promuovere e coordinare le iniziative volte ad agevolare la conoscenza e la comprensione del Modello da parte dei Destinatari.

6.2. Formazione del personale

L'attività di formazione è finalizzata a promuovere la conoscenza della normativa di cui al D.Lgs. n. 231/2001. Tale conoscenza implica che venga fornito un quadro esaustivo della normativa stessa, dei risvolti pratici che da essa discendono, nonché dei contenuti e principi su cui si basano il Modello. Tutti i Soggetti Apicali ed i Soggetti Sottoposti sono pertanto tenuti a conoscere, osservare e rispettare tali contenuti e principi contribuendo alla loro attuazione.

Per garantire l'effettiva conoscenza del Modello, del Codice Etico e dei Controlli Aziendali da adottare per un corretto svolgimento delle attività, sono pertanto previste specifiche attività formative obbligatorie rivolte ai Soggetti Apicali ed ai Soggetti Sottoposti di Teleippica, da erogare con differenti modalità a seconda dei soggetti destinatari ed in coerenza con le modalità di erogazione dei piani formativi in uso presso la Società.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale A

I reati contro la Pubblica Amministrazione
e l'Amministrazione della Giustizia
(artt. 24, 25 e 25 decies del D.Lgs. 231/01)

Teleippica SRL

INDICE

1. Premessa

La presente Parte Speciale riguarda i reati previsti dagli articoli 24, 25 e 25 decies del D.Lgs. 231/01 (di seguito anche i "***Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia***") ed, in particolare, i comportamenti che devono essere tenuti dagli amministratori e dai componenti degli altri organi sociali, dai dirigenti e dai dipendenti di Teleippica S.r.l. (di seguito "*Teleippica*" o "*Società*"), ovunque essi operino, nonché dai collaboratori e consulenti esterni di Teleippica, indipendentemente dalla qualificazione giuridica del loro rapporto con la Società, dai fornitori e da coloro che intrattengono, in via diretta ed indiretta, contatti e rapporti di natura contrattuale e non contrattuale (es. licenze, autorizzazioni, procedimenti giudiziari) con la Pubblica Amministrazione o l'Amministrazione delle Giustizia (di seguito, in breve, anche "P.A.") e con soggetti ad essa assimilati in nome e/o per conto o su incarico della Società (qui di seguito i "Destinatari").

Per Pubblica Amministrazione si intende, in estrema sintesi, l'insieme di enti e soggetti pubblici (Stato, Ministeri, Regioni, Province, Comuni, ecc.), ma anche le persone giuridiche di diritto privato che esercitano funzioni pubbliche, la Pubblica Amministrazione di Stati Esteri, nonché tutti quei soggetti che possano essere qualificati come tali in base alla vigente legislazione (organismi di diritto pubblico, concessionari, organismi di vigilanza o di controllo, ecc.).
L'art. 357 c.p. definisce come pubblico ufficiale "*chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa*", specificando che "*agli stessi effetti, è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autorizzativi e caratterizzata dalla formazione e dalla manifestazione della volontà della Pubblica Amministrazione e dal suo svolgersi per mezzo dei poteri autorizzativi e certificativi*".

I 'pubblici poteri' qui in rilievo sono: il potere legislativo, il potere giudiziario e quelli riconducibili alla 'pubblica funzione amministrativa'.

Il potere legislativo trova la sua connotazione nell'attività diretta alla produzione di provvedimenti aventi valore di legge (es. leggi e atti del Governo aventi forza di legge, ecc.). E' definito Pubblico Ufficiale, in quanto svolge la "pubblica funzione legislativa", chiunque, a livello nazionale o comunitario, partecipi all'esplicazione di tale potere. I soggetti pubblici a cui normalmente può ricondursi l'esercizio di tali tipologie di poteri sono a mero titolo esemplificativo il Parlamento, il Governo, le Regioni, le Province e le Istituzioni dell'Unione Europea aventi competenze legislative rilevanti nell'ambito dell'ordinamento nazionale.

Il potere giudiziario consiste nell'applicazione del diritto oggettivo, interpretandone le norme e rendendole operanti nel caso concreto. Svolgono tale tipo di funzione, pertanto, tutti i soggetti che partecipano sia alla vera e propria attività giurisdizionale in senso proprio, sia a quella amministrativa collegata alla stessa, quali a titolo esemplificativo magistrati, pubblici ministeri, membri della Corte di Giustizia e della Corte dei Conti Comunitarie.

I poteri riconducibili alla **"*pubblica funzione amministrativa*"**, sono il potere deliberativo, il potere autorizzativo ed il potere certificativo della Pubblica Amministrazione:

- ***Potere deliberativo della P.A.***: è quello relativo alla "*formazione e manifestazione della volontà della Pubblica Amministrazione*", e cioè qualsiasi attività che concorra a definire il potere stesso. Rientra in tale definizione, ad esempio, il potere di una commissione di un Bando di aggiudicare una gara ad un partecipante;

- ***Potere autoritativo della P.A.***: si identifica in tutte quelle attività che permettono alla Pubblica Amministrazione di realizzare i suoi fini mediante veri e propri comandi. Questo ruolo della PA è, ad esempio, facilmente individuabile nel potere della stessa di rilasciare concessioni ai privati. Alla luce di queste considerazioni, possono essere qualificati come "pubblici ufficiali" tutti i soggetti preposti ad esplicare tale potere;

- ***Potere certificativo della P.A.***: si concretizza nell'attività di ricognizione, da parte di un pubblico agente, avente per oggetto la rappresentazione come certa di una determinata situazione.

Diversamente, l'art. 358 c.p., attribuisce la qualifica di "***incaricato di un pubblico servizio***" (di seguito "Incaricato di Pubblico Servizio") a tutti "*coloro i quali, a qualunque titolo, prestano un pubblico servizio*", intendendosi per tale "*un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima e con esclusione dello svolgimento di semplici mansioni d'ordine e della prestazione di opera meramente materiale*".
E', pertanto, un Incaricato di Pubblico Servizio colui il quale svolge un servizio pubblico, che si caratterizza per l'assenza dei poteri di natura certificativa, autorizzativa e deliberativa, propri della pubblica funzione. Esempi di Incaricato di Pubblico Servizio sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati.
Nella concessione di pubblico servizio, il concessionario sostituisce la Pubblica Amministrazione nell'erogazione del servizio, ossia nello svolgimento dell'attività diretta al soddisfacimento dell'interesse collettivo. Il concessionario di pubblico servizio, è quindi chiamato a realizzare i compiti istituzionali dell'ente pubblico concedente, con il conseguente trasferimento delle potestà pubbliche.

2. I reati di cui agli artt. 24 e 25 e 25 decies del D.Lgs. 231/2001 - Esempi delle modalità di commissione

Viene riportato di seguito il testo delle disposizioni del Codice Penale espressamente richiamate dagli artt. 24 e 25 e 25 decies del D.Lgs. 231/2001 (qui di seguito anche il "Decreto") unitamente ad un breve commento delle singole fattispecie.

- **Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, co. 2 c.p.):**

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

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

"La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee".

- **Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-*ter* c.p.):**

"I. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.
II. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
III. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

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

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

- **Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-*ter* c.p.):**

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

- **Concussione (art. 317 c.p.):**

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

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

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

- **Corruzione per un atto contrario ai doveri d'ufficio (artt. 319 – 319-*bis* c.p.).**

- **Articolo 319 - Corruzione per un atto contrario ai doveri d'ufficio:**
  "Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da quattro a otto anni".
- **Articolo 319-bis - Circostanze aggravanti:**
  "La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene".

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

"I. Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da quattro a dieci anni.
II. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da cinque a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni."

- **Induzione indebita a dare o promettere utilità (Art. 319-*quater* c.p.)**

"I. Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da tre a otto anni.

II. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni".

- **Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.):**

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

- **Istigazione alla corruzione (art. 322 c.p.):**

"I. Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo.
II. Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.
III. La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.
IV. La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319."

- **Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-*bis* c.p.):**

"I. Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:
1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.
II. Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:
1) alle persone indicate nel primo comma del presente articolo;
2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica finanziaria.

III. Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

In considerazione dell'attività svolta, la Società ha ritenuto **rilevanti** le seguenti fattispecie di reato, di cui viene riportato un breve commento.

- ***Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, co. 2 c.p.):***

Il reato di truffa sopra riportato appartiene al novero dei delitti contro il patrimonio, punibili indipendentemente dalla circostanza che il soggetto leso o tratto in inganno sia lo Stato od altro Ente Pubblico.

Ai fini della responsabilità amministrativa degli enti prevista dal Decreto in relazione al reato di cui all'articolo in commento, è necessario che tale delitto sia posto in essere dai soggetti apicali e/o dai soggetti sottoposti ai danni dello Stato, di altro Ente Pubblico o dell'Unione Europea.

Tale reato può realizzarsi quando, ad esempio, nella predisposizione di documenti o dati da trasmettere agli Enti Pubblici competenti, si forniscano informazioni non veritiere od incomplete supportate da artifici e raggiri, al fine di ottenere un ingiusto profitto per l'ente o il versamento di imposte/contributi inferiori a quelli realmente dovuti.

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

Il reato si configura nel caso in cui la truffa menzionata al precedente punto sia posta in essere per conseguire indebitamente contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri Enti pubblici o delle Comunità Europee.

- ***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, manipolando o duplicando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro Ente Pubblico.

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

Il reato si configura nel caso in cui, taluno, estraneo alla Pubblica Amministrazione, dopo aver ricevuto finanziamenti o contributi o sovvenzioni da parte dello Stato o di altro ente pubblico o delle Comunità Europee destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non utilizzi dette somme ottenute per gli scopi cui erano destinate. Tenuto conto che il momento della commissione del reato coincide con il mancato utilizzo o la destinazione ad altri impieghi delle erogazioni, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non vengono destinati alle finalità per cui sono stati erogati.

- ***Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-ter c.p.):***

Il reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, si ottengano indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre

erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità Europee.

- ***Corruzione (artt. 318 - 319 - 319bis - 319ter - 319quater - 320 - 322 - 322bis, c.p.):***

Le norme di cui sopra assumono rilevanza ai fini del presente Modello in ragione del dettato codicistico, nella misura in cui prevede conseguenze penali anche in capo al soggetto "corruttore".

I reati di corruzione impropria e propria (artt. 318 e 319 c.p., sopra riportati) si configurano nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio[4] si faccia dare o promettere (anche attraverso induzione), per sé o per altri, denaro o altra utilità per compiere, omettere o ritardare atti della sua funzione ovvero per compiere atti contrari ai suoi doveri di ufficio.
I reati di corruzione impropria o propria si configurano nel caso in cui l'indebita offerta o promessa sia formulata con riferimento ad atti – conformi alla funzione o contrari ai doveri d'ufficio - compiuti dal pubblico ufficiale o dall'incaricato di pubblico servizio. Ad esempio, sussiste la commissione dei reati in questione quando il pubblico ufficiale, dietro corrispettivo, velocizzi o abbia velocizzato una pratica, la cui evasione è di propria competenza (corruzione impropria), oppure quando ometta o attenuti l'irrogazione di sanzioni conseguenti ad eventuali rilievi (corruzione propria per un atto contrario ai propri doveri d'ufficio).

Per quanto riguarda il reato di corruzione in atti giudiziari, di cui all'art. 319-*ter* sopra riportato, esso si configura nel caso in cui taluno offra o prometta ad un pubblico ufficiale[5] denaro o altra utilità per compiere o aver compiuto, omettere o aver omesso, ritardare o aver ritardato atti del suo ufficio ovvero per compiere o aver compiuto atti contrari ai suoi doveri di ufficio: tutto ciò allo scopo precipuo di favorire o danneggiare una parte in un processo civile, penale o amministrativo. Potrà dunque essere chiamato a rispondere del reato di cui all'art. 319-*ter* il soggetto apicale che corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro pubblico ufficiale), al fine di ottenere la positiva definizione di un procedimento giudiziario.

Le ipotesi di corruzione indicate agli articoli 318, 319, 319-*ter* e 319-*quater* 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 concusso subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio[6].

Come anticipato, l'esposizione delle fattispecie di reato di corruzione sopra operata acquista rilevanza ai fini del presente Modello in ragione delle disposizioni contenute nel Codice Penale, che

[4] Per quanto riguarda l'applicabilità anche agli incaricati di un pubblico servizio delle fattispecie delittuose previste agli articoli 318 e 319 c.p. vale la pena di riportare di seguito quanto statuito dall'art. 320 c.p., espressamente richiamato all'art. 25, 4° comma, del d.lgs. 231/2001: "*Le disposizioni degli artt. 318 e 319 si applicano anche all'incaricato di un pubblico servizio. In ogni caso, le pene sono ridotte in misura non superiore a un terzo".*

[5] L'esclusione dell'applicabilità di tale fattispecie di reato agli incaricati di pubblico servizio sembra pacifica considerato che l'art. 320 c.p. nel richiamo delle ipotesi di corruzione poste in essere dall'incaricato di pubblico servizio si limita a citare gli articoli 318 e 319 c.p. e, viceversa, non ricomprende l'art. 319-*ter*.

[6] In altri termini, "*mentre nella corruzione (...) i soggetti trattano pariteticamente con manifestazioni di volontà convergenti sul «pactum sceleris», nella concussione il dominus dell'illecito è il pubblico ufficiale il quale, abusando della sua autorità e del suo potere, costringe con minaccia o induce con la frode il privato a sottostare all'indebita richiesta, ponendolo in una situazione che non offre alternative diverse dalla resa*" (così: Cass. Pen. Sent. 2265 del 24 febbraio 2000).

disciplinano le conseguenze negative previste in capo al *corruttore* del pubblico ufficiale o dell'incaricato del pubblico servizio.

In vero, a questo proposito, l'art. 321 c.p. (Pene per il corruttore) prevede espressamente che: "*Le pene stabilite nel primo comma dell'articolo 318* (Corruzione Impropria), *nell'articolo 319* (Corruzione Propria), *nell'articolo 319-bis* (Circostanze Aggravanti), *nell'articolo 319-ter* (Corruzione in atti giudiziari), *e nell'articolo 320* (Corruzione di persona incaricata di un pubblico servizio*), in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità*".
Inoltre, secondo quanto previsto all'art. 322 c.p. (Istigazione alla corruzione), le pene specificamente previste agli articoli 321 e 322, 1° e 2° comma, c.p., sono applicabili al corruttore non solo nell'ipotesi in cui il reato di corruzione sia stato effettivamente consumato attraverso la dazione di denaro od altra utilità, ma anche nell'ipotesi in cui il reato sia rimasto nella fase del tentativo perché, ad esempio, il pubblico ufficiale o l'incaricato di pubblico servizio non hanno accettato tale dazione.

Sotto il profilo delle finalità contemplate dal D. Lgs. n. 231/2001, è ravvisabile una responsabilità dell'ente nell'ipotesi in cui i soggetti apicali o soggetti sottoposti offrano o promettano ad un pubblico ufficiale od ad un incaricato di pubblico servizio[7] denaro o altra utilità per compiere o aver compiuto, omettere o aver omesso, ritardare o aver ritardato atti rientranti nella sua funzione ovvero per compiere o aver compiuto atti contrari ai suoi doveri di ufficio e dalla commissione di uno di tali reati sia derivato all'ente un interesse o un vantaggio.

Qualora, viceversa, i soggetti apicali o soggetti sottoposti abbiano tentato di corrompere il pubblico ufficiale o l'incaricato di pubblico servizio, ma questi ultimi non abbiano accettato la promessa o la dazione di denaro o di altra utilità (articoli 321, 1° e 2° comma, c.p.), ai fini della punibilità dell'ente sotto il profilo del D. Lgs. n. 231/2001, occorrerà verificare concretamente se, ciononostante, derivi a tale soggetto giuridico un interesse od un vantaggio.

A completamento dell'esame del reato di corruzione previsto dall'art. 25 del Decreto, vale la pena rilevare che il corruttore o l'istigatore alla corruzione soggiace alle medesime pene indicate agli articoli 321 e 322 c.p. sopra riportati qualora il denaro o l'utilità sono offerti o promessi:

a) "*ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;*
b) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
c) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
d) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
e) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio"[8]*;*

[7] L'esclusione dell'applicabilità di tale fattispecie di reato agli incaricati di pubblico servizio sembra pacifica considerato l'art. 320 c.p. (v. nota precedente) nel richiamo delle ipotesi di corruzione poste in essere dall'incaricato di pubblico servizio si limita a citare gli articoli 318 e 319 c.p. e, viceversa, non ricomprende l'art. 319-*ter* c.p.
[8] Così testualmente: art. 322-*bis*, 1° comma, c.p.

f) "a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali"[9].

- ***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.)***

"Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha facoltà di non rispondere, è punito con la reclusione da due a sei anni".

Il reato si configura mediante l'induzione, a seguito di violenza, minaccia ovvero offerta o promessa di denaro o altre utilità, del soggetto avente facoltà di non rispondere, a non rendere dichiarazioni - ossia ad avvalersi di tale facoltà - o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Giudice o Pubblico Ministero).

I destinatari della condotta sono, dunque, gli indagati e gli imputati (anche in procedimento connesso o in un reato collegato), ai quali è riconosciuta dall'ordinamento la facoltà di non rispondere.

Quanto alle modalità tipiche della realizzazione della condotta, l'induzione rilevante al fine della consumazione del reato, si realizza mediante l'azione con la quale un soggetto esplica un'influenza sulla psiche di un altro soggetto, determinandolo a tenere un certo comportamento, esplicata attraverso i mezzi tassativamente indicati dalla norma, ovvero minaccia, violenza o promessa di denaro o altra utilità.

E' richiesto inoltre per la realizzazione degli elementi costitutivi della fattispecie che:
- la persona indotta non abbia reso dichiarazioni o le abbia rese mendaci;
- l'agente si rappresenti che la persona da lui indotta - con le modalità indicate dalla norma - a non rendere dichiarazioni o a renderle non veritiere, aveva la facoltà di non rispondere.

Ne consegue pertanto che, ai fini della responsabilità amministrativa dell'ente prevista dal D. Lgs. n. 231/2001, rileva la condotta dei soggetti apicali o soggetti sottoposti, non solo nei confronti dei pubblici ufficiali e degli incaricati di pubblico servizio dello Stato italiano, bensì anche nei confronti dei pubblici ufficiali e degli incaricati di pubblico servizio delle Comunità Europee, degli Stati membri, degli Stati esteri e delle organizzazioni pubbliche internazionali.

[9] Così testualmente: art. 322-*bis*, 2° comma, n. 2, c.p.

3. Le sanzioni previste in relazione agli artt. 24-25 e 25 Decies del Decreto

Si riporta di seguito una tabella riepilogativa delle sanzioni a carico dell'Ente previste agli articoli 24, 25 e 25 decies del Decreto qualora, per effetto della commissione dei reati indicati al precedente paragrafo 2, da parte dei soggetti apicali e/o dei soggetti sottoposti, derivi all'Ente un interesse o un vantaggio.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
• Malversazione a danno dello Stato (art. 316-*bis* c.p.) • Indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.) • Truffa commessa a danno dello Stato o di altro ente pubblico (art. 640, comma 2 n. 1 c.p.) • Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.) • Frode informatica commessa a danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.)	Fino a 500 quote Da 200 a 600 quote se profitto di rilevante entità, ovvero se il danno derivato è di particolare gravità	Si applicano le sanzioni interdittive previste dall'art. 9, co. 2, lett. c), d) ed e) del Decreto: c) divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) divieto di pubblicizzare beni o servizi.
• Corruzione per atto d'ufficio (art. 318 c.p.) • Istigazione alla corruzione (art. 322, commi 1 e 3, c.p.) • Pene per il corruttore (art. 321 c.p.)	Fino a 200 quote, anche se i delitti sono commessi dalle persone indicate negli articoli 320 e 322-*bis* c.p.	
• Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) • Corruzione in atti giudiziari (art. 319-ter, comma 1 c.p.)	Da 200 a 600 quote, anche se i delitti sono commessi dalle persone indicate negli articoli 320 e 322-*bis* c.p.	Si applicano tutte le sanzioni interdittive previste dall'art. 9, co. 2 del Decreto, per un periodo non inferiore a un anno: a) l'interdizione dall'esercizio della attività; b) la sospensione o la revoca

• Pene per il corruttore (321 c.p.) • Istigazione alla corruzione (ipotesi di cui all'art. 322, commi 2 e 4, c.p.).		delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.
• Concussione (art. 317 c.p.) • Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) aggravata ex art. 319-bis c.p., quando dal fatto l'ente ha conseguito un profitto di rilevante entità • Corruzione in atti giudiziari se dal fatto deriva ingiusta condanna (art. 319-ter, comma 2, c.p.) • Induzione indebita a dare o promettere utilità (319-*quater* c.p.) • Pene per il corruttore (321 c.p.).	Da 300 a 800 quote (anche se i delitti sono commessi dalle persone indicate negli articoli 320 e 322-*bis* c.p.)	Si applicano le sanzioni interdittive previste dall'art. 9, co. 2 del Decreto, per un periodo non inferiore a un anno: a) l'interdizione dall'esercizio della attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la Pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.
• Articolo 377-bis, c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Fino a 500 quote	Nessuna

Oltre alle sanzioni sopra citate vanno in ogni caso considerate le ulteriori sanzioni previste dal Decreto:

- la confisca del prezzo o del profitto del reato, sempre disposta con la sentenza di condanna, salvo che per la parte che può essere restituita al danneggiato;

- la pubblicazione della sentenza di condanna, che può essere disposta, secondo le modalità di cui all'art. 36 c.p., quando nei confronti dell'Ente viene applicata una sanzione interdittiva.

4. Le aree a potenziale rischio reato diretto e le aree c.d. "strumentali"

Ai fini della commissione dei reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia è necessaria l'instaurazione di rapporti di natura contrattuale e non contrattuale (ad es. licenze, autorizzazioni) con Pubblici Ufficiali, Incaricati di Pubblico Servizio appartenenti alla Pubblica Amministrazione, agli enti pubblici o ai soggetti ad essi assimilati facenti parte dello Stato Italiano, delle Comunità Europee e degli Stati esteri.
Nel corso dell'attività di analisi condotta nell'ambito delle varie Direzioni/Funzioni aziendali, Teleippica ha provveduto ad individuare le aree a rischio reato costituite da:

- aree a rischio "***reato diretto***", ossia nel cui ambito sono poste in essere attività, che per effetto di contatti diretti con i Pubblici Ufficiali o Incaricati di Pubblico Servizio, comportino il rischio di commissione di uno o più dei reati contro la Pubblica Amministrazione (qui di seguito "***Aree a Rischio Reato Diretto***");
- aree a rischio c.d. "***strumentali***" alla realizzazione dei reati contro la Pubblica Amministrazione, ossia aree che, comportando la gestione di strumenti di tipo finanziario o mezzi sostitutivi, possono supportare la commissione dei reati nelle Aree a Rischio Reato Diretto attraverso la creazione di fondi o provviste (qui di seguito "***Aree a Rischio Reato Strumentali***").

Si riporta, di seguito, l'indicazione delle Aree a Rischio individuate dalla Società in relazione ai Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia:

Aree a Rischio Reato Diretto:

- Gestione dei rapporti con il Mipaaf;
- Gestione dei rapporti con altre Pubbliche Amministrazioni;
- Gestione del contenzioso;
- Acquisizione e gestione di finanziamenti pubblici per la formazione del personale.

Aree a Rischio Reato Strumentali:

- Selezione ed assunzione del personale;
- Amministrazione del personale;
- Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza;
- Acquisto di beni e servizi;
- Amministrazione, contabilità e bilancio;
- Tesoreria;
- Gestione contenuti editoriali;
- Gestione sistemi informativi;
- Pianificazione e Controllo.

Eventuali integrazioni delle suddette aree a rischio reato potranno essere proposte al Consiglio di Amministrazione di Teleippica, sia dall'Organismo di Vigilanza che dagli altri organi di controllo della Società, per effetto dell'evoluzione dell'attività di impresa e conseguentemente di eventuali

modifiche dell'attività svolta dalle singole Direzioni/Funzioni.

Nell'ambito di ciascuna **Area a Rischio Reato Diretto o Strumentale, gestita totalmente o parzialmente da Teleippica**, sono state individuate le c.d. "attività sensibili", ossia quelle attività al cui svolgimento è connesso il rischio di commissione dei reati con i soggetti sopra definiti come Pubblica Amministrazione.
Sono state, inoltre, identificate le funzioni o i ruoli aziendali coinvolti nell'esecuzione di tali attività "sensibili". L'individuazione dei ruoli/funzioni non deve considerarsi, in ogni caso, tassativa atteso che ciascun soggetto aziendale potrebbe in linea teorica essere coinvolto.
Sono stati individuati, altresì, in via esemplificativa, con riferimento a ciascuna area, alcune potenziali modalità di realizzazione dei reati ed i principali controlli previsti con riferimento alle attività poste in essere nelle Aree a Rischio.

Invece, nell'ambito di ciascuna **Area a Rischio Reato Diretto o Strumentale, esternalizzata ad altre società**, anche facenti parte del Gruppo SNAI, sono state individuate le relative attività "sensibili" e i principali controlli preventivi posti in essere in relazione alle aree "a rischio", o porzioni di esse, esternalizzate.

Di seguito è riepilogato il quadro in precedenza esposto.

4.1. Le Aree potenzialmente a Rischio Reato Diretto gestite parzialmente o totalmente da Teleippica. Le attività "sensibili", i ruoli aziendali coinvolti, le potenziali modalità di realizzazione dei reati ed i presidi di controllo esistenti

- **Gestione dei rapporti con il Mipaaf**

Attività sensibili:

- Autorizzazione della documentazione afferente alla partecipazione a bandi pubblici per l'ottenimento dei diritti radio - televisivi;
- Gestione dei rapporti con il Mipaaf in merito ad atti, dichiarazioni ed adempimenti relativi a bandi pubblici per l'ottenimento dei diritti radio – televisivi;
- Gestione dei rapporti con il Mipaaf in merito i all'attività di collaudo da parte dello stesso;
- Gestione della rendicontazione al Mipaaf;
- Gestione dei ricorsi e/o contenziosi con il Mipaaf.

Processi e ruoli aziendali coinvolti:

- Gestione degli atti ed adempimenti derivanti dalla convenzione stipulata con l'Ente Concedente e delle verifiche ispettive correlate – Amministratore Delegato;
- Gestione degli atti ed adempimenti derivanti dalla convenzione stipulata con l'Ente Concedente e delle verifiche ispettive correlate – Responsabile Funzione Service Management / Responsabile Funzione Esercizio/ Responsabile Funzione Produzione/ Responsabile Funzione Progettazione e Post Produzione/ Responsabile Funzione Rete.

Reati astrattamente ipotizzabili ed esemplificazioni delle modalità di commissione dei reati:

- ***Corruzione per l'esercizio della funzione (art. 318 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto d'ufficio.

- ***Corruzione per un atto contrario ai doveri d'ufficio (artt. 319 – 319-bis c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto contrario ai doveri d'ufficio.
- ***Indebita induzione a dare o promettere utilità (art. 319-quater):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, ad un pubblico ufficiale o incaricato di pubblico servizio, su induzione da parte di quest'ultimo, al fine di ottenere il compimento di un atto contrario ai doveri d'ufficio.
- ***Istigazione alla corruzione (art. 322 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento, ovvero per omettere o ritardare il compimento di un atto d'ufficio, qualora la dazione o la promessa non sia accettata.
- ***Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, co. 2 c.p.):*** Realizzazione di artifizi o raggiri da cui deriva, mediante induzione in errore, un ingiusto profitto, con altrui danno, quando il fatto è commesso ai danni dello Stato o di altro ente pubblico.

Presidi di controllo esistenti:
Per ciò che concerne la presente Area a Rischio Reato e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.
In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio Reato devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Previsione, all'interno del Codice Etico, dell'invito a mantenere un comportamento improntato a criteri di lealtà, trasparenza, correttezza ed integrità nei rapporti con qualsiasi Autorità Pubblica;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei rapporti con la Pubblica Amministrazione e con il Mipaaf;
- Formale identificazione dei soggetti autorizzati ad intrattenere rapporti con il Mipaaf;
- Svolgimento delle attività secondo i principi di separazione delle funzioni e nel rispetto della normativa applicabile;
- Sistematica revisione e formale autorizzazione, da parte dei soggetti delegati, della documentazione predisposta per gli adempimenti nei confronti della Pubblica Amministrazione;
- Definizione, tramite contratto, delle modalità di determinazione del corrispettivo spettante a Teleippica per lo svolgimento dell'attività radio televisiva;
- Formalizzazione e sistematica archiviazione dei verbali e della documentazione prodotta in seguito ai rapporti intercorsi con l'Ente Concedente.

- **Gestione dei rapporti con altre pubbliche Amministrazioni**

Attività sensibili:

- Autorizzazione di atti, adempimenti e dichiarazioni relativi a dipendenti e collaboratori presso gli Istituti Previdenziali e Assistenziali (es. INPS, INAIL, ecc.);
- Autorizzazione di atti, adempimenti e dichiarazioni relativi all'assunzione di personale anche con riferimento alle categorie protette o la cui assunzione è agevolata;

- Autorizzazione di atti e adempimenti relativi alla dichiarazione dei redditi o dei sostituti d'imposta o di altre dichiarazione funzionali alla liquidazione dei tributi in genere;
- Gestione dei rapporti con i funzionari delle Autorità incaricati di effettuare verifiche, ispezioni ed accertamenti e trasmissione della relativa documentazione (es. Agenzia delle Entrate, INPS, INAIL, Comuni, ecc.).

Processi e ruoli aziendali coinvolti:

- Gestione dei rapporti, degli adempimenti e delle dichiarazioni relativi a tematiche giuslavoristiche – Amministratore Delegato.
- Gestione dei rapporti, degli adempimenti e delle dichiarazioni relativi a tematiche fiscali - Amministratore Delegato.

Reati astrattamente ipotizzabili ed esemplificazioni delle modalità di commissione dei reati:

- ***Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, co. 2 c.p.):*** Realizzazione di artifizi o raggiri da cui deriva, mediante induzione in errore, un ingiusto profitto, con altrui danno, quando il fatto è commesso ai danni dello Stato o di altro ente pubblico.
- ***Corruzione per l'esercizio della funzione (art. 318 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto d'ufficio.
- ***Corruzione per un atto contrario ai doveri d'ufficio (artt. 319 – 319-bis c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto contrario ai doveri d'ufficio.
- ***Indebita induzione a dare o promettere utilità (art. 319-quater):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, ad un pubblico ufficiale o incaricato di pubblico servizio, su induzione da parte di quest'ultimo, al fine di ottenere il compimento di un atto contrario ai doveri d'ufficio.
- ***Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto d'ufficio da parte di un pubblico impiegato, ovvero il compimento di un atto contrario ai doveri d'ufficio da parte di Incaricato di Pubblico Servizio.
- ***Istigazione alla corruzione (art. 322 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento, ovvero per omettere o ritardare il compimento di un atto d'ufficio, qualora la dazione o la promessa non sia accettata.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Reato e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio Reato devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Previsione, all'interno del Codice Etico, dell'invito a mantenere un comportamento improntato a criteri di lealtà, trasparenza, correttezza ed integrità nei rapporti con qualsiasi Autorità Pubblica;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei rapporti con qualsiasi Autorità Pubblica;

- Formale identificazione dei soggetti aziendali autorizzati a intrattenere rapporti con la Pubblica Amministrazione (es. INPS, INAIL, Agenzia delle Entrate, ecc.);
- Segregazione di funzioni tra chi predispone i documenti da inoltrare alla PA e chi verifica, autorizza e firma i suddetti documenti;
- Sistematica revisione e formale autorizzazione, da parte dei soggetti delegati, della documentazione predisposta per gli adempimenti nei confronti della Pubblica Amministrazione;
- Formalizzazione e sistematica archiviazione dei verbali e della documentazione prodotta in seguito ai rapporti intercorsi con la PA.

- **Gestione del contenzioso**

Attività sensibili:

- Definizione ed autorizzazione delle strategie societarie in relazione alla gestione dei contenziosi;
- Definizione ed autorizzazione di accordi transattivi;
- Sottoscrizione di atti, adempimenti e dichiarazioni relativamente ai contenziosi e/o agli accordi transattivi in essere (es. fiscali, amministrativi, civili, giuslavoristici, ecc.).

Processi e ruoli aziendali coinvolti:

- Definizione ed autorizzazione delle strategie societarie in relazione ai contenziosi e agli accordi transattivi - Amministratore Delegato / Consiglio di Amministrazione.

Reati astrattamente ipotizzabili ed esemplificazioni delle modalità di commissione dei reati:

- ***Corruzione in atti giudiziari (art. 319-ter c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, effettuata anche mediante un consulente legale o un terzo, al fine di favorire la Società, ovvero per danneggiare un'altra parte in un procedimento giudiziario civile, penale o amministrativo.
- ***Corruzione per l'esercizio della funzione (art. 318 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto d'ufficio.
- ***Corruzione per un atto contrario ai doveri d'ufficio (artt. 319 – 319-bis c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto contrario ai doveri d'ufficio.
- ***Indebita induzione a dare o promettere utilità (art. 319-quater):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, ad un pubblico ufficiale o incaricato di pubblico servizio, su induzione da parte di quest'ultimo, al fine di ottenere il compimento di un atto contrario ai doveri d'ufficio.
- ***Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento di un atto d'ufficio da parte di un pubblico impiegato, ovvero il compimento di un atto contrario ai doveri d'ufficio da parte di Incaricato di Pubblico Servizio.
- ***Istigazione alla corruzione (art. 322 c.p.):*** Dazione o promessa di denaro o di altra utilità, diretta o indiretta, al fine di ottenere il compimento, ovvero per omettere o ritardare il compimento di un atto d'ufficio, qualora la dazione o la promessa non sia accettata.

- ***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.):*** Il reato previsto potrebbe dirsi integrato qualora un soggetto riferibile alla Società (ivi inclusi i consulenti legali esterni che agiscono in nome e per conto della Società) ponga in essere, con violenza, minaccia o promessa di denaro o altra utilità, misure atte ad indurre le persone che sono tenute a rendere all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale (es. testimonianze) a rendere dichiarazioni non veritiere sul conto, ad esempio, di attività illecite degli amministratori/o altri dipendenti della Società.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Reato e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio Reato devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Previsione, all'interno del Codice Etico, della collaborazione attiva con le Autorità Pubbliche nel corso di qualsiasi indagine o verifica ispettiva;
- Individuazione dei soggetti autorizzati a rappresentare la Società nel corso di contenziosi e accordi transattivi (es. fiscali, amministrativi, civili, giuslavoristici, ecc.).
- Sistematico coinvolgimento del vertice aziendale in merito alla definizione delle linee guida da seguire per la gestione delle controversie e/o per la definizione di accordi transattivi;
- Formale autorizzazione delle strategie societarie in relazione alla gestione dei contenziosi e degli accordi transattivi;
- Informativa regolare e periodica verso il vertice aziendale in merito ai contenziosi in essere.

4.2. Le Aree potenzialmente a Rischio Reato Strumentali gestite parzialmente o totalmente da Teleippica. Le attività "sensibili", i ruoli aziendali coinvolti ed i presidi di controllo esistenti

a. Selezione ed assunzione del personale

Attività sensibili:

- Assunzione del candidato.

Processi e ruoli aziendali coinvolti:

- Gestione delle attività connesse all'assunzione del personale - Amministratore Delegato / Consiglio di Amministrazione.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Definizione delle responsabilità e dei livelli autorizzativi nell'ambito del processo di assunzione;
- Formalizzazione del contratto di assunzione e autorizzazione dello stesso secondo i suddetti livelli autorizzativi;
- Regolamentazione, all'interno del contratto di assunzione, della retribuzione spettante al neoassunto, dell'eventuale previsione di premi di produttività o altri elementi di retribuzione variabile, nonché dell'utilizzo di eventuali benefit aziendali;
- Previsione, all'interno del contratto di assunzione, delle clausole di accettazione del Modello 231 e del Codice Etico di Teleippica;
- Autorizzazione, da parte del procuratore abilitato, di qualsiasi modifica alle condizioni contrattuali non derivante dalla contrattazione collettiva.

b. Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza

Attività sensibili:

- Definizione ed approvazione delle iniziative legate all'omaggistica;
- Gestione delle ospitalità e delle spese di rappresentanza.

Processi e ruoli aziendali coinvolti:

- Definizione ed approvazione delle iniziative legate all'omaggistica – Amministratore Delegato;
- Gestione delle ospitalità e delle spese di rappresentanza – Procuratore Abilitato.

Presidi di controllo esistenti:
Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.
In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Previsione, all'interno del Codice Etico, del divieto tassativo di erogare omaggi, liberalità o altre cortesie a soggetti pubblici;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dell'omaggistica, delle ospitalità e delle spese di rappresentanza;
- Previsione ed autorizzazione, in base alle deleghe vigenti, di un budget degli omaggi, delle ospitalità e delle spese di rappresentanza;
- Formale identificazione dei soggetti responsabili all'autorizzazione degli omaggi;
- Autorizzazione preventiva ai fini della concessione di ospitalità e spese di rappresentanza;
- Verifica delle spese di rappresentanza ed ospitalità sostenute e sottoposizione delle stesse a specifica autorizzazione da parte di un Procuratore Abilitato.

c. Acquisto di beni e servizi

Attività sensibili:

- Autorizzazione degli ordini di acquisto;
- Emissione del benestare al pagamento.

Processi e ruoli aziendali coinvolti:

- Autorizzazione degli approvvigionamenti sulla base del sistema di deleghe e procure vigente – Responsabile Area Richiedente/ Procuratore abilitato;
- Emissione al benestare al pagamento – Tutti i referenti interessati.

Presidi di controllo esistenti:
Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.
In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei flussi di approvvigionamento;
- Previsione, all'interno di tutti i contratti stipulati, di clausole di accettazione, da parte della controparte, del Modello 231 e del Codice Etico di Teleippica;
- Segregazione di funzioni tra chi attesta la ricezione del bene/servizio e approva la fattura e chi effettua/autorizza il pagamento;

- Approvazione dei contratti di approvvigionamento secondo i livelli autorizzativi definiti dalla Società in base agli importi degli stessi;
- Formale autorizzazione degli acquisti in "extra-budget";
- Formale identificazione delle modalità di gestione degli acquisti "a carattere d'urgenza";
- Verifica a posteriori, da parte del procuratore abilitato, circa tutti gli acquisti "a carattere d'urgenza"
- Monitoraggio delle prestazioni ricevute tramite verifica dell'allineamento con quanto concordato a livello contrattuale;
- Verifica della ricezione dei beni e servizi e del rispetto delle relative condizioni contrattuali prima di apporre il benestare al pagamento.

d. Tesoreria

Attività sensibili:

- Autorizzazione degli Ordini di Pagamento;
- Gestione della piccola cassa.

Processi e ruoli aziendali coinvolti:

- Autorizzazione degli Ordini di Pagamento - Procuratore abilitato;
- Gestione della piccola cassa.

Controlli esistenti:

Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Segregazione delle funzioni tra chi predispone gli ordini di pagamento e chi li approva;
- Autorizzazione degli ordini di pagamento da parte del procuratore abilitato, nel rispetto delle procure in essere;
- Verifica della corrispondenza tra fattura e ordine/contratto;
- Verifica, da parte del procuratore abilitato, precedentemente al rilascio dell'autorizzazione al pagamento, dei seguenti aspetti:
  - completa ed accurata compilazione della proposta di pagamento;
  - presenza di una fattura autorizzata (presenza del benestare al pagamento della fattura);
  - corrispondenza tra il beneficiario indicato nella proposta di pagamento e il fornitore indicato in fattura;
  - corrispondenza tra l'importo della proposta di pagamento e quello indicato in fattura;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione della piccola cassa;
- Definizione del limite di importo massimo della piccola cassa (giacenza massima);
- Definizione delle tipologie di spese che possono essere sostenute tramite cassa, del relativo ammontare massimo e dei soggetti abilitati ad autorizzarle;

- Verifica di corrispondenza tra le spese autorizzate ed i relativi giustificativi di spesa;
- Definizione delle modalità operative di reintegro della piccola cassa;
- Riconciliazione periodica, fisico-contabile, dei valori di cassa.

e. Gestione dei contenuti editoriali

Attività sensibili:

- Definizione ed approvazione del contratto giornalistico e del prezzo finale di acquisto del servizio;
- Monitoraggio degli adempimenti contrattuali;
- Utilizzo e sfruttamento di materiale editoriale pubblicato presso i media (canali televisivi, radio, ecc.).

Processi e ruoli aziendali coinvolti:

- Gestione dei servizi giornalistici - Area Editoriale.
- Pubblicazione di materiale editoriale - Area Editoriale.

Controlli esistenti:

Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei contenuti editoriali;
- Previsione, all'interno del Codice Etico, che tutti i rapporti con le Terze Parti siano ispirati a principi di lealtà, correttezza e onestà;
- Previsione, all'interno di tutti i contratti stipulati, di clausole di accettazione, da parte delle controparte, del Modello 231 e del Codice Etico di Teleippica;
- Segregazione delle funzioni tra chi definisce gli importi dei contratti e chi approva i contratti editoriali;
- Autorizzazione dei contratti editoriali da parte del procuratore abilitato, nel rispetto delle procure in essere;
- Verifica degli adempimenti, degli obblighi e delle condizioni contrattuali posti in capo ai consulenti esterni (es. giornalisti, ecc.);
- Archiviazione delle liberatorie nonché di tutti i documenti relativi ai contenuti editoriali messi in onda.

f. Gestione sistemi informativi

Attività sensibili:

- Gestione della sicurezza fisica e logica delle informazioni aziendali elettroniche o in forma digitale;
- Gestione della configurazione delle componenti software ed hardware installate sulle postazioni di lavoro;
- Gestione degli accessi alle apparecchiature informatiche, alla rete aziendale, alle applicazioni ed ai sistemi ed alle reti telematiche;
- Protezione dei dispositivi rimovibili (es. hard disk esterno; pen drive);
- Acquisizione, sviluppo e manutenzione dei sistemi informatici;
- Gestione dei cambiamenti degli applicativi aziendali;
- Gestione del flusso informativo verso Enti Pubblici, mediante strumenti informatici;
- Gestione delle informazioni e dei dati custoditi presso gli archivi informatici;
- Gestione degli incidenti e dei problemi di sicurezza informatica su dati ed informazioni.

Processi e ruoli aziendali coinvolti:

- Gestione delle componenti software/hardware, delle reti aziendali, dei flussi informativi informatici e della custodia dei dati – Area ICT.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei componenti software/hardware, delle reti aziendali, dei flussi informativi informatici e della custodia dei dati;
- Previsione, all'interno del Codice Etico, che tutti i rapporti con le Terze Parti siano ispirati a principi di lealtà, correttezza e onestà;
- Formale definizione delle responsabilità relative all'utilizzo di Internet, dei servizi di Posta Elettronica e della rete aziendale quali strumenti a fini esclusivi di lavoro;
- Esistenza di controlli automatici volti a bloccare una sessione inattiva o ad effettuare il log-off di terminali inattivi connessi alla rete aziendale;
- Formale definizione delle procedure volte a limitare l'effetto di software dannosi e ripristinare il corretto funzionamento dei sistemi: sull'intera rete (personal computer e server) è installato un software antivirus ed è previsto un controllo di accesso ad internet tramite Websense;
- L'utilizzo dei servizi informatici aziendali richiede un codice di identificazione personale (user-id) ed una parola chiave segreta (password), che non può essere ceduta a terzi neppure temporaneamente;
- Formale definizione dei requisiti della password, in termini di lunghezza minima, scadenza, history, lockout e complessità della password;

- Formale definizione dei processi di ingresso di un nuovo dipendente, di dimissioni o di cambio ufficio, relativamente ai profili di accesso ai sistemi informativi;
- Review periodica delle utenze di accesso alle applicazioni aziendali;
- L'utilizzo di internet, quale strumento ai fini esclusivi di lavoro, è autorizzato solo attraverso la rete di trasmissione dati aziendale;
- La casella di posta è assegnata al dipendente (che è responsabile del suo corretto utilizzo) quale strumento ai fini esclusivi di lavoro. L'account di e-mail viene assegnato al dipendente su richiesta del proprio Responsabile e può essere configurato solo su un PC client di posta;
- Definizione di controlli volti a garantire l'integrità e l'autenticità dei dati trasmessi su reti pubbliche, quali ad esempio la firma digitale;
- Definizione di controlli volti a vietare l'accesso abusivo al proprio sistema telematico al fine di alterare e /o cancellare dati e/o informazioni;
- Definizione di controlli volti a vietare l'utilizzo abusivo di codici, parole chiave o altri mezzi idonei all'accesso a un sistema telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- Previsione di divieto di procedere all'installazione di qualsiasi software o hardware senza preventiva autorizzazione;
- Esistenza di firewall;
- Gestione delle connessioni da remoto verso la intranet aziendale attraverso il protocollo standard VPN (Virtual Private Network);
- Le macchine server sono custodite all'interno di sale server il cui accesso è limitato;
- L'utilizzo di dispositivi rimovibili (floppy disk, cd rom, cd riscrivibili, nastri magnetici, chiavi USB) può avvenire solo previa autorizzazione.

4.3. Le Aree potenzialmente a Rischio Reato Diretto o Strumentali totalmente o parzialmente esternalizzate

Di seguito è riportato l'elenco delle Aree potenzialmente a Rischio Reato Diretto o Strumentali, o porzioni di esse, e delle relative attività "sensibili" esternalizzate ad altre società, anche facenti parte del Gruppo Snai.

a) Gestione dei rapporti con il Mipaaf e con altre pubbliche Amministrazioni

Attività sensibili:

- Predisposizione ed invio di documentazione afferente alla partecipazione ai bandi pubblici per l'ottenimento dei diritti radio-televisivi;
- Predisposizione ed invio di documentazione connessa alla gestione dei rapporti con il Mipaaf;
- Predisposizione ed invio di dichiarazioni dei redditi, dei sostituti d'imposta e di altre dichiarazioni funzionali alla liquidazione dei tributi in genere;
- Predisposizione ed invio dei dati relativi a dipendenti e collaboratori agli Istituti Previdenziali ed Assistenziali (es. INPS, INAIL);
- Predisposizione ed invio delle dichiarazioni contributive e versamento dei contributi previdenziali e assistenziali (CUD);
- Supporto nella gestione dei rapporti con gli uffici competenti (es. Direzione Provinciale del Lavoro, Ispettorato del Lavoro, ecc.), in materia di assunzione e impiego di personale appartenente a categorie protette o la cui assunzione è agevolata (diversamente abili, ecc);
- Supporto ed assistenza nella contrattazione con i rappresentanti sindacali aziendali e nazionali.

b) Gestione del contenzioso

Attività sensibili:

- Supporto nella gestione dei contenziosi e degli accordi transattivi (fiscali, amministrativi, civili, giuslavoristici, ecc.);
- Selezione dei consulenti legali esterni;
- Monitoraggio sugli onorari e sull'attività svolta dai consulenti legali esterni.

c) Acquisizione e gestione di finanziamenti pubblici per la formazione del personale

Attività sensibili:

- Richiesta dei finanziamenti per la formazione del personale;
- Organizzazione dei corsi di formazione per il personale;
- Gestione dei finanziamenti per la formazione del personale;
- Attività di rendicontazione per i finanziamenti ricevuti relativi alla formazione del personale e richiesta di recupero dei fondi.

d) Selezione e assunzione del personale

Attività sensibili:

- Definizione dei criteri di selezione del personale in relazione al profilo ricercato;
- Selezione del personale.

e) Amministrazione del personale

Attività sensibili:

- Gestione dell'anagrafica dipendenti;
- Rilevazione delle presenze;
- Elaborazione dei cedolini del personale dipendente e parasubordinato;
- Elaborazione delle dichiarazioni contributive previdenziali e assistenziali;
- Gestione note spese e trasferte.

f) Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza

Attività sensibili:

- Gestione delle iniziative legate all'omaggistica.

g) Acquisto di beni e servizi

Attività sensibili:

- Rilevazione del fabbisogno di beni e/o servizi ed emissione della richiesta di acquisto;
- Selezione del fornitore;
- Ricezione beni e servizi;
- Selezione dei consulenti;
- Definizione e monitoraggio degli onorari dei consulenti.

h) Gestione contenuti editoriali

Attività sensibili:

- Selezione dei consulenti (giornalisti);
- Definizione e monitoraggio degli onorari dei consulenti.

i) Amministrazione, contabilità e bilancio

Attività sensibili:

- Gestione della Contabilità Clienti: Gestione dell'anagrafica dei clienti ed emissione delle fatture attive;

- Gestione della Contabilità Fornitori: Gestione dell'anagrafica fornitori, registrazione e contabilizzazione della fatture passive;
- Tenuta delle scritture obbligatorie e dei Libri (IVA, Libro cespiti, Inventari, ecc.);
- Gestione delle attività propedeutiche alla predisposizione del Bilancio (scritture di rettifica e chiusura) e delle situazioni infrannuali;
- Predisposizione delle situazioni infrannuali;
- Predisposizione del Bilancio Annuale;
- Collaborazione con gli Organi di Controllo (Collegio Sindacale, Società di Revisione, ecc.).

g. Tesoreria

Attività sensibili:

- Gestione degli incassi e dei pagamenti;
- Gestione dei conti correnti bancari e/o postali;
- Gestione delle riconciliazioni bancarie;
- Coordinamento della pianificazione finanziaria di Teleippica con quella della Capogruppo Snai;
- Gestione dei rapporti con gli istituti di credito e finanziari per la negoziazione delle condizioni di accesso al credito e delle relative forme di garanzia;
- Gestione di operazioni finanziarie di straordinaria amministrazione.

h. Pianificazione e controllo

Attività sensibili:

- Predisposizione del budget dei costi annuale;
- Produzione della reportistica e rendicontazione;
- Analisi degli scostamenti ed identificazione degli interventi da implementare (revisione degli obiettivi).

Controlli preventivi applicabili a tutte le Aree potenzialmente a Rischio Reato Diretto o Strumentali totalmente o parzialmente esternalizzate:

- Formale definizione della politica per la esternalizzazione delle attività della Società, anche mediante individuazione dei metodi per la valutazione del livello delle prestazioni del fornitore (S.L.A.);
- Formalizzazione di contratti di outsourcing nell'ambito dei quali è prevista:
  - l'identificazione dei servizi da erogare ed il relativo livello di servizio atteso (S.L.A.);
  - l'inserimento di clausole specifiche nell'ambito delle quali la società mandataria si impegna a rispettare i presidi di controllo previsti nel proprio Modello (ove adottato dalla società mandataria) nonché i principi ispiratori del Modello di Teleippica;
  - l'inserimento di clausole specifiche nell'ambito delle quali le società si impegnano, nei confronti l'una dell'altra, al rispetto più rigoroso dei propri Modelli (ove adottati), con

particolare riguardo alle aree dei Modelli che presentano rilevanza ai fini delle attività gestite mediante contratto di *outsourcing* e della sua esecuzione; con tali clausole, si impegnano altresì a darsi reciprocamente notizia di eventuali violazioni, che dovessero verificarsi e che possano avere attinenza con il contratto e/o la sua esecuzione e più in generale, ad astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che possano integrare una qualsivoglia fattispecie di reato contemplata dal Decreto;

- l'applicazione di sanzioni (ivi inclusa l'eventuale risoluzione del contratto) in caso di violazioni alle suddette prescrizioni.

5. Principi e regole di comportamento nei rapporti con la Pubblica Amministrazione e l'Amministrazione della Giustizia

Tutte le attività ricomprese nelle Aree a Rischio Reato Diretto e Strumentali devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure di Teleippica, nonché le regole contenute nel presente Modello.
In generale, il sistema di organizzazione, gestione e controllo della Società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, e tracciabilità.
Nello svolgimento delle attività sopra descritte ed, in generale, delle proprie funzioni, gli organi sociali, gli amministratori, i dipendenti, i procuratori di Teleippica, nonché i collaboratori e tutte le altre controparti contrattuali, devono conoscere e rispettare:

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

5.1. Principi generali di comportamento

I Destinatari della presente Parte Speciale coinvolti nelle attività elencate nei paragrafi precedenti devono rispettare principi e norme di comportamento di seguito dettate, nel rispetto degli obblighi normativi, delle procedure aziendali e del Codice Etico di Teleippica.
Come stabilito dal Codice Etico, i rapporti tra la Società e la Pubblica Amministrazione devono essere condotti in conformità alla legge e nel rispetto dei principi di lealtà, correttezza, trasparenza e verificabilità.
E' assolutamente vietato:

- mettere in atto comportamenti tali da esporre la Società ad una delle fattispecie di reato previste dagli artt. 24, 25 e 25 decies del Decreto;
- mettere in atto comportamenti tali da favorire l'attuarsi di fattispecie di reato previste dagli artt. 24, 25 e 25 decies del Decreto;
- promettere, offrire o acconsentire all'elargizione di denaro o altre utilità (beni materiali, servizi, ecc.) a Pubblici Ufficiali o Incaricati di Pubblico Servizio italiani ed esteri, o a loro familiari, che possano influenzare l'indipendenza del giudizio o indurre ad assicurare un vantaggio per la Società;
- accordare vantaggi di qualsiasi natura (promessa di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione, italiana o straniera, che possano determinare le stesse conseguenze previste al punto precedente;
- promettere, offrire o acconsentire alla distribuzione di omaggi e regalie non dovuti ovvero che non siano di modico valore;
- destinare le erogazioni pubbliche, i contributi o i finanziamenti agevolati ottenuti da organismi pubblici nazionali o comunitari ad attività diverse rispetto a quelle originariamente pattuite;
- esibire dichiarazioni, documenti, dati e informazioni volutamente artefatti o incompleti agli organismi pubblici nazionali, comunitari o esteri;
- esibire dichiarazioni, documenti, dati, informazioni volutamente artefatti o incompleti per conseguire indebitamente erogazioni pubbliche o contributi o finanziamenti agevolati;

- coartare, in qualsiasi forma e con qualsiasi modalità, la volontà di rispondere all'Autorità Giudiziaria di soggetti chiamati a rendere dichiarazioni o di indurre questi ad avvalersi della facoltà di non rispondere;
- indurre, in qualsiasi modo, i soggetti chiamati a rendere dichiarazioni di fronte all'Autorità Giudiziaria, a rendere dichiarazioni non veritiere;
- elargire, offrire o promettere denaro, omaggi, regali o altri vantaggi a persone chiamate a rendere dichiarazioni di fronte all'Autorità Giudiziaria.

A tal fine, è necessario il rispetto dei seguenti principi:

- presentare le comunicazioni dovute e gli eventuali documenti richiesti da membri della Pubblica Amministrazione o da soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio in modo completo, veritiero e tempestivo;
- adottare un comportamento improntato ai principi di diligenza, onestà, trasparenza, competenza, conformità alla legge, buona fede, massima correttezza ed integrità in relazione a qualsiasi attività da intraprendersi nell'ambito di ogni attività aziendale;
- garantire il rispetto dei principi di correttezza, trasparenza, e buona fede in qualsiasi rapporto professionale che si intraprenda con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- operare, in ogni rapporto con la Pubblica Amministrazione, nel rispetto della legge e della corretta prassi commerciale e tenere condotte collaborative al fine di non ostacolare o ritardare l'esercizio delle relative funzioni, anche in sede di eventuali ispezioni ed investigazioni;
- riferire prontamente all'Organismo di Vigilanza di eventuali situazioni di irregolarità.

6. Compiti dell'Organismo di Vigilanza

Fermi restando i compiti e le funzioni dell'Organismo di Vigilanza statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, previsti dal Decreto;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune, al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV svolge in piena autonomia le proprie attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici e/o a campione sulle attività connesse ai reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia al fine di verificare la corretta implementazione delle stesse in relazione alle regole previste nel Modello. A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.
L'OdV comunica i risultati della propria attività di controllo relativamente ai reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia al Consiglio di Amministrazione e al Collegio Sindacale, secondo quanto previsto nella Parte Generale del Modello.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale B

Reati Societari
(Art. 25-ter D. Lgs 231/2001)

TELEIPPICA SRL

INDICE

1. Premessa

La presente Parte Speciale riguarda i reati previsti dall'articolo 25-*ter* del D.Lgs. n. 231/2001, introdotto dal D.Lgs. 11 aprile 2002, n. 61, e successive modifiche e integrazioni.

La presente Parte Speciale concerne, in particolare, i comportamenti che devono essere tenuti dai soggetti – Amministratori, dirigenti e dipendenti di Teleippica S.r.l. (di seguito "*Teleippica*" o "*Società*"), anche per il tramite di fornitori e consulenti che svolgono la propria prestazione all'interno della Società, indipendentemente dalla qualificazione giuridica del loro rapporto con la Società - che sono coinvolti nei processi e nelle attività sensibili ed operano pertanto nelle Aree a Rischio Reato (qui di seguito i "Destinatari").

Tutti i Destinatari della presente Parte Speciale del Modello sono tenuti ad adottare comportamenti conformi a quanto di seguito formulato, al fine di prevenire la commissione dei reati individuati nell'ambito della normativa di riferimento.

2. I delitti di cui all'art. 25-ter del D.Lgs. 231/2001 – Esempi delle modalità di commissione

L'articolo 25-*ter* del D.Lgs. n. 231/2001 richiama i Reati Societari, di seguito, elencati:

- False comunicazioni sociali (artt. 2621 c.c.);
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto d'interessi (art.2629– bis c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Corruzione tra privati (art. 2635 c.c., oggetto della specifica Parte Speciale "B1");
- Illecita influenza sull'Assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

In particolare, in considerazione dell'attività svolta, la Società ha ritenuto rilevanti le seguenti fattispecie di reato, di cui viene riportato il testo integrale, unitamente ad un breve commento.

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

"Salvo quanto previsto dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non corrispondenti al vero ancorché oggetto di valutazioni, ovvero omettono informazioni 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 in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni.
La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.
La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio non superiore all'1 per cento.
In ogni caso, il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.
Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone

giuridiche e delle imprese da sei mesi a sei anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa".

Il reato si realizza ad opera di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori i quali, con l'intenzione di ingannare i soci o il pubblico ed al fine di conseguire per sé o per altri un ingiusto profitto, espongono 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 omettono informazioni, 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 in errore i destinatari sulla predetta situazione.

Quanto al soggetto attivo del reato, si noti che i commentatori sottolineano che questa qualifica "*è collegata allo svolgimento delle attività tipiche*", a prescindere dall'investitura formale. Pertanto, "*sarà responsabile anche l'amministratore di fatto, il direttore generale di fatto, il sindaco di fatto, il liquidatore di fatto*" [1]. Inoltre, Confindustria ha specificato che tale reato può essere "*posto in essere dai livelli sottostanti, segnatamente dai responsabili delle varie funzioni aziendali (...). E' altresì possibile che (...) siano commessi da "sottoposti" dei responsabili di funzione, dotati di un certo potere discrezionale, ancorché circoscritto. In tali casi, il reato potrà dirsi consumato solo se la falsità sia colpevolmente condivisa dai soggetti "qualificati" che, nel recepire il dato falso, lo fanno proprio inserendolo nella comunicazione sociale. Se non vi è tale partecipazione cosciente e volontaria da parte dei soggetti "qualificati" il reato non è configurabile"*[2].

Si precisa che le informazioni false od omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene; la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società, per conto di terzi.
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%, ovvero una variazione del patrimonio netto non superiore all'1%.
In ogni caso, il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10% da quella corretta.

Deve farsi presente che, nella struttura dell'illecito in esame, è previsto il conseguimento di un "ingiusto profitto" a favore del soggetto autore dell'illecito medesimo o di soggetti terzi. A fronte di tale previsione, la dottrina si è interrogata se, anche nel caso specifico, possa configurarsi la responsabilità amministrativa dell'ente ai sensi del D.Lgs. n. 231/2001, posto che l'art. 5, comma 1, di tale legge dispone che "*L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio*". Nel caso disciplinato dall'art. 2621 c.c., invece, non viene menzionato il conseguimento di alcun interesse o vantaggio dell'ente, ma solo il conseguimento di un ingiusto profitto del soggetto attivo o di terzi.

[1] Ciccia, *I nuovi reati societari e finanziari*, Napoli, 2006, pag. 27.
[2] Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex d.lgs. 231/2001*, ed. 31 marzo 2008, *sub* art. 2621, 2622 c.c. e 173-*bis* TUF.

Senza entrare nel merito del dibattito dottrinale tra i sostenitori della tesi per cui sarebbe sufficiente la sussistenza soltanto dell'interesse dell'ente, e non anche del vantaggio[3], e coloro che, invece, sostengono la necessità della ricorrenza di entrambi questi elementi[4], si deve comunque rilevare che, ai fini della configurabilità della responsabilità amministrativa dell'ente, lo stesso deve avere goduto almeno di un interesse dalla commissione del reato in esame.

Alla luce di quanto sopra, l'ambito di applicazione della responsabilità amministrativa della persona giuridica risulta alquanto limitato in relazione alla fattispecie contemplata nell'art. 2621 c.c.

Fermo restando quanto sopra, vale comunque la pena rilevare che la ricorrenza dell'effettivo interesse o vantaggio dell'ente andrà valutata in concreto, avuto riguardo del caso specifico e delle modalità con cui il reato si è realizzato, con la conseguenza che costituisce buona norma di corretta e scrupolosa gestione e amministrazione societaria la messa in atto di tutte le cautele ed i rimedi volti ad evitare il rischio di commissione del reato *de quo*.

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

"Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazione o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni 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 in errore i destinatari sulla predetta situazione, cagionano un danno patrimoniale alla società, ai soci o ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Si procede a querela anche se il fatto integra altro delitto, ancorché aggravato, a danno del patrimonio di soggetti diversi dai soci e dai creditori, salvo che sia commesso in danno dello Stato, di altri enti pubblici e delle Comunità Europee.
Nel caso di società soggette alle disposizioni della parte IV, titolo III, capo II, del testo unico di cui al D.Lgs. 24 febbraio 1998, n. 58, e successive modificazioni, la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è ricedibile d'ufficio.
La pena è da due a sei anni se, nelle ipotesi di cui al terzo comma, il fatto cagiona un grave nocumento ai risparmiatori.
Il nocumento si considera grave quando abbia riguardato un numero di risparmiatori superiore allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT ovvero se sia

[3] Bassi – Epidendio, *Enti e responsabilità da reato*, Milano, 2006, pag. 162; Aparo – Fucito, *I Reati presupposto*, in *Trattato di diritto penale dell'impresa – La responsabilità degli enti*, diretto da Amato, Milano, 2009, pag. 470 e ss., in cui gli Autori sostengono che "*la circostanza che uno degli elementi costitutivi dell'incriminazione sia rappresentato «dall'intenzione di ingannare i soci o il pubblico» e dal «fine di conseguire per sé o per altri un ingiusto profitto» non vale di per sé ad escludere la sussistenza di un interesse esclusivo e concomitante della società*".
[4] Cordero, *Procedura penale*, VI ed., Milano, 2001; Pulitanò, *La responsabilità amministrativa per i reati delle persone giuridiche*, in *Enc. Dir.*, 2002, app. V, agg.; Cocco, *L'illecito degli enti dipendente da reato e il ruolo dei modelli di prevenzione*, in *Riv. It. Dir. Proc. Pen*., 2004; Falcinelli, in *La responsabilità degli enti*, a cura di Presutti – Bernasconi – Fiorio, Milano, 2008, pag. 269 ss.

consistito nella distruzione o riduzione del valore dei titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo.
La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.
La punibilità per i fatti previsti dal primo e terzo comma è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico 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, differiscono in misura non superiore al 10 per cento da quella corretta.
Nei casi previsti dai commi settimo e ottavo, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa".

Tale reato si configura quando gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di una società, con l'intenzione di ingannare i soci o il pubblico ed al fine di conseguire per sé o per altri un ingiusto profitto, cagionano un danno patrimoniale alla società, ai soci e/o ai creditori esponendo – nei bilanci, nelle relazioni o in altre comunicazioni sociali previste dalla legge, dirette ai soci e al pubblico – fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero omettendo informazioni 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 in errore i destinatari sulla predetta situazione.

Analogamente alla previsione di cui al punto precedente, la punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi, mentre è esclusa se le falsità od omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene.

La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico o di esercizio, al lordo delle imposte, non superiore al 5%, ovvero una variazione del patrimonio netto non superiore all'1%.
In ogni caso, il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10% da quella corretta.

Trattasi di un reato di danno di natura delittuosa, che si differenzia dal reato di cui all'art. 2621 c.c. per il fatto che ai fini della sua configurabilità è necessario che alla condotta illecita del soggetto attivo del reato sia seguito un danno in pregiudizio del soggetto passivo.

In relazione al soggetto attivo dell'illecito, valgono le osservazioni svolte *sub* art. 2621 c.c.

Analogamente, quanto all'interesse dell'ente ed alla conseguente configurabilità di una sua responsabilità amministrativa, si rinvia alle considerazioni svolte in merito all'art. 2621 c.c., aggravate in questo caso dal fatto che, al fine della commissione del reato, è necessario altresì un danno per l'ente stesso. Ne consegue, pertanto, che nella fattispecie in questione appare alquanto improbabile la possibilità di una commissione dell'illecito nell'interesse dell'ente.

Il reato in commento è punibile a querela, salvo che si tratti di società quotate, in relazione alle quali è procedibile d'ufficio.

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

"*Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci, o ad altri organi sociali, sono puniti con la sanzione amministrativa pecuniaria fino a Euro 10.329.*
Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.
La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'unione Europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del testo unico di cui al D.Lgs. 24 febbraio 1998 n. 58".

Il comma 1 della norma in esame punisce a titolo di illecito amministrativo l'ostacolo o l'impedimento - realizzati attraverso l'occultamento di documenti o con altri idonei artifici - delle funzioni di controllo legalmente attribuite ai soci o ad altri organi sociali (ad esempio, collegio sindacale).

Le stesse funzioni ottengono una protezione (mediata) sul piano penale solo qualora dal fatto derivi un danno ai soci, il cui patrimonio è il bene oggetto di tutela della disposizione contenuta nel comma 2.

Si tratta di illecito proprio degli amministratori (anche di fatto), per la cui configurabilità è necessario e sufficiente il dolo generico.

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

"*Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno*".

La norma disciplina un reato di natura dolosa proprio degli amministratori e tutela l'interesse alla integrità ed effettività del capitale sociale, con garanzia dei creditori e dei terzi.

La fattispecie si realizza nel momento in cui gli amministratori, nonostante non ricorra alcuna delle legittime ipotesi di riduzione del capitale sociale legislativamente tipizzate, restituiscono ai soci gli

apporti destinati a far parte del capitale sociale ovvero liberano gli stessi soci dall'obbligo di eseguire il singolo conferimento.
Il reato può essere realizzato attraverso due modalità di condotta:

- la restituzione dei conferimenti ai soci, che comporta uno svuotamento del capitale sociale precedentemente costituito e può avvenire in modo palese, con trasferimento dell'oggetto del conferimento senza adeguato corrispettivo, oppure, in forma simulata (sia totale che parziale), qualora avvenga un pagamento a fronte di prestazioni inesistenti o di valore inferiore a quanto versato oppure, ancora, con qualsiasi comportamento che possa integrare gli estremi di altre figure di reato (ad esempio, una distribuzione di utili fittizia o di acconti dividendo effettuata con somme indebitamente prelevate dal capitale sociale);
- la liberazione dell'obbligo di eseguire i conferimenti, che impedisce la regolare costituzione del capitale.

Oggetto di restituzione sono i conferimenti, cioè gli apporti patrimoniali (prestazioni in denaro, crediti e beni in natura) cui i soci si sono obbligati per costituire la dotazione necessaria per lo svolgimento dell'attività sociale.

- **Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)**

"*Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge esser distribuite, sono puniti con l'arresto fino ad un anno.*
La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato".

La disposizione, che disciplina un reato proprio degli amministratori, mira a tutelare i creditori sociali dalla "*menomazione delle loro garanzie, costituite dal capitale e dalle riserve obbligatorie*"[5].
"*La condotta di ripartizione indica un'attività che determini l'effettivo trasferimento di ricchezza dal patrimonio sociale ad altro soggetto*"[6].
Oggetto materiale del riparto sono utili o acconti su utili non effettivamente conseguiti[7] o destinati per legge a riserva, ovvero riserve, anche non costituite con utili, che non possono per legge essere distribuite[8].

[5] Musco, *I nuovi reati societari*, Milano, pag. 164.
[6] Napoleoni, *La tutela penale del capitale sociale e delle riserve*, in *Trattato diretto da Galgano*, XXV, pag. 232.
[7] Si noti che "*la dottrina civilistica è concorde nel ritenere che per integrare il reale conseguimento, presupposto della distribuibilità dell'utile, l'utile stesso non necessariamente deve essere «liquido», essendo sufficiente che sia «effettivo»*" (L. Alibrandi, *sub art. 2627 c.c.*, in *I Reati Societari, Commentario aggiornato alla legge 28 dicembre 2005 n. 262 sulla tutela del risparmio*, a cura di A. Lanzi e A. Cadoppi, Milano, 2007, pag. 118
[8] Tra le riserve che, per legge, non possono essere distribuite, si possono annoverare: (i) riserva legale (art. 2430 c.c.); (ii) riserva di sovrapprezzo azioni nei limiti stabiliti dallo stesso articolo (art. 2431 c.c.); (iii) riserva *ex* art. 2423, 4° comma, c.c.; (iv) riserve di rivalutazione monetaria costituite in corrispondenza di specifici provvedimenti di rivalutazione (art. 2426, n. 8-*bis*), c.c.); (v) riserve per azioni proprie emesse dalla società (art. 2357-*ter*, 3° comma, c.c.); (vi) riserve costituite in esecuzione dell'art. 2426, 2° comma, c.c., in caso di partecipazioni iscritte per la prima volta in base al metodo del patrimonio netto.

Il reato è punibile a titolo sia di dolo che di colpa.

Il comma 2 prevede una speciale causa di non punibilità, consistente nella restituzione degli utili o nella ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio.

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

"*Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
Il risarcimento del danno ai creditori prima del giudizio estingue il reato".

La norma ha ad oggetto un reato proprio degli amministratori e mira alla tutela del capitale sociale in funzione di garanzia delle ragioni dei creditori, che potrebbero rimanere lesi nei propri diritti di credito a seguito di operazioni poste in essere dagli amministratori stessi (*i.e.* riduzione del capitale sociale, fusione, scissione) con il deliberato proposito di eludere le prescrizioni legislative previste in materia.
Le condotte incriminate consistono nell'effettuare:

- riduzioni del capitale sociale al di fuori delle ipotesi legislativamente previste o, addirittura, al di sotto del limite legale;
- fusioni tra due società, una delle quali si trovi in una situazione di dissesto finanziario, con la conseguenza che, nell'ipotesi di procedura concorsuale, i creditori della società patrimonialmente solida vengono scientemente o dolosamente messi in concorso con i creditori della società insolvente;
- scissioni da precedenti organismi societari, da cui derivi un danno per i creditori.

Il danno sussiste quando, a seguito della condotta illecita posta in essere dagli amministratori, i creditori si trovano in una posizione deteriore rispetto a quella che avevano prima dell'effettuazione dell'operazione.

L'elemento soggettivo è rappresentato dal dolo generico, ovvero dalla consapevolezza e volontà di violare specifiche norme e di provocare un danno ai creditori.
L'ultimo comma prevede, poi, una speciale causa di non punibilità, consistente nel risarcimento del danno ai creditori prima del giudizio.

Il reato è perseguibile solo dietro querela della persona offesa.

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

"*Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno*".

Oggetto di tutela della presente norma incriminatrice è l'integrità del capitale sociale.

Trattasi di reato proprio degli amministratori e dei soci conferenti, per la configurabilità del quale è sufficiente il dolo generico.

Le condotte tipiche punite dalla disposizione sono le seguenti:

- attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni o di crediti ovvero del patrimonio della società.

A questo proposito, giova rilevare che, sia in sede di costituzione della società per azioni, sia in sede di aumento del capitale sociale (qualora tali operazioni vengano poste in essere mediante il conferimento di beni o crediti), nonché in sede di trasformazione da una società di persone ad una di capitali, è necessaria la relazione di stima ai sensi dell'articolo 2343 c.c., fatta eccezione per i casi previsti dall'art. 2343-*ter* c.c.
In altri termini, l'esperto nominato ha l'incarico di attestare che il valore dei conferimenti è superiore al valore delle azioni o quote emesse oppure, in caso di trasformazione societaria, l'esatto valore del patrimonio sociale che, comunque, non deve essere inferiore al capitale minimo legislativamente previsto in relazione alla singola forma societaria prescelta.

Essendo la relazione di stima un incarico legislativamente previsto a carico dell'esperto designato dal Tribunale e non prevedendo la norma di cui all'art. 2343 c.c. alcuna conseguenza a carico degli amministratori nell'ipotesi in cui non attuino gli obblighi previsti a loro carico ai sensi del terzo comma della medesima disposizione, da più parti in dottrina ci si è chiesti a quale titolo gli amministratori potrebbero rispondere del reato oggetto di commento. A questo proposito, vale la pena di precisare che, secondo una (ormai risalente) dottrina, la responsabilità degli amministratori deriverebbe dall'art. 40, comma 2, c.p., in forza del quale "*Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo*". Vi è da dire comunque che parte della dottrina più recente ha sottoposto a dura critica tale impostazione, in considerazione del fatto che l'obbligo di controllo legislativamente posto a carico degli amministratori ai sensi dell'art. 2343 c.c., è necessariamente successivo al momento in cui si avrebbe la consumazione del reato.

- **Illecita influenza sull'Assemblea (art. 2636 c.c.)**

"*Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni*".

Il reato, che può essere commesso da chiunque, si integra quando, allo scopo di conseguire, per sé o per altri, un ingiusto profitto (dolo specifico), si determina con atti simulati o con frode una maggioranza in assemblea che non vi sarebbe stata senza i voti illecitamente ottenuti.

Anche se si tratta di un reato comune, è indispensabile che, ai fini dell'applicazione del D.Lgs. n. 231/2001, lo stesso sia stato commesso dagli amministratori, direttori generali o liquidatori della società, o da persone sottoposte alla loro vigilanza.

3. Le sanzioni previste dall'art 25-ter del D.Lgs. n. 231/01

Si riporta, di seguito, una tabella riepilogativa delle sanzioni previste dall'art. 25-*ter* del D.Lgs. n. 231/2001 a carico dell'ente, qualora, per effetto della commissione dei reati sopra indicati, derivi allo stesso ente un interesse o un vantaggio.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
False comunicazioni sociali (art. 2621 c.c.)	Da 200 a 300 quote	Nessuna
False comunicazioni sociali in danno della società, dei soci e dei creditori (art. 2622 c.c.)	Da 300 a 660 quote (art. 2622, comma 1, c.c.) Da 400 a 800 quote (art. 2622, comma 3, c.c.)	Nessuna
Impedito controllo (art. 2625 c.c.)	Da 200 a 360 quote	Nessuna
Indebita restituzione dei conferimenti (art. 2626 c.c.)	Da 200 a 360 quote	Nessuna
Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)	Da 200 a 260 quote	Nessuna
Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)	Da 200 a 360 quote	Nessuna
Operazioni in pregiudizio dei creditori (art. 2629 c.c.)	Da 300 a 660 quote	Nessuna
Formazione fittizia del capitale (art. 2632 c.c.)	Da 200 a 360 quote	Nessuna
Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)	Da 300 a 660 quote	Nessuna
Illecita influenza sull'assemblea (art. 2636 c.c.)	Da 300 a 660 quote	Nessuna

4. Le Aree a potenziale Rischio Reato, le attività "sensibili", le funzioni o i ruoli aziendali coinvolti ed i controlli a presidio

Con riferimento alle fattispecie richiamate dall'art. 25-*ter* del D.Lgs. n. 231/2001 considerate applicabili alla Società (come sopra individuate), in considerazione della specifica attività svolta da Teleippica, sono state individuate le seguenti aree a rischio:

- Acquisto di beni e servizi;
- Amministrazione, Contabilità e Bilancio;
- Tesoreria.

Nell'ambito di ciascuna **Area a Rischio Reato, gestita totalmente o parzialmente da Teleippica**, sono state individuate le c.d. "attività sensibili", ossia quelle attività al cui svolgimento è connesso il rischio di commissione dei reati in oggetto.
Sono state, inoltre, identificate le funzioni o i ruoli aziendali coinvolti nell'esecuzione di tali attività "sensibili". L'individuazione dei ruoli/funzioni non deve considerarsi, in ogni caso, tassativa atteso che ciascun soggetto aziendale potrebbe in linea teorica essere coinvolto.
Sono stati individuati, altresì, in via esemplificativa, con riferimento a ciascuna area, alcune potenziali modalità di realizzazione dei reati ed i principali controlli previsti con riferimento alle attività poste in essere nelle Aree a Rischio.

Invece, nell'ambito di ciascuna **Area a Rischio Reato esternalizzata ad altre società**, anche facenti parte del Gruppo Snai, sono state individuate le relative attività "sensibili" ed i principali controlli preventivi posti in essere in relazione alle aree "a rischio", o porzioni di esse, esternalizzate.

Di seguito è riepilogato il quadro in precedenza esposto.

Eventuali integrazioni delle Aree a potenziale Rischio Reato potranno essere proposte al Consiglio di Amministrazione dall'OdV e dagli altri organi di controllo della Società, per effetto dell'evoluzione dell'attività di impresa e conseguentemente ad eventuali modifiche dell'attività svolta dalle singole Direzioni/Funzioni.

4.1 Le Aree potenzialmente a Rischio Reato gestite parzialmente o totalmente da Teleippica. Le attività "sensibili", i ruoli aziendali coinvolti, le potenziali modalità di realizzazione dei reati ed i presidi di controllo esistenti

a) Acquisto di beni e servizi

Attività sensibili:

- Autorizzazione degli ordini di acquisto;
- Emissione del benestare al pagamento.

Processi e ruoli aziendali coinvolti:

- Autorizzazione degli approvvigionamenti sulla base del sistema di deleghe e procure vigente – Responsabile Area Richiedente/ Procuratore abilitato;
- Emissione del benestare al pagamento – Tutti i referenti interessati.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei flussi di approvvigionamento;
- Previsione, all'interno di tutti i contratti stipulati, di clausole di accettazione, da parte della controparte, del Modello 231 e del Codice Etico di Teleippica;
- Approvazione dei contratti di approvvigionamento secondo i livelli autorizzativi definiti dalla Società in base agli importi degli stessi;
- Monitoraggio delle prestazioni ricevute tramite verifica dell'allineamento con quanto concordato a livello contrattuale;
- Verifica della ricezione dei beni e servizi e del rispetto delle relative condizioni contrattuali prima di apporre il benestare al pagamento;
- Segregazione di funzioni tra chi attesta la ricezione del bene/servizio e approva la fattura e chi effettua/autorizza il pagamento;
- Formale autorizzazione degli acquisti in "extra-budget";
- Formale identificazione delle modalità di gestione degli acquisti "a carattere d'urgenza";
- Verifica a posteriori, da parte del procuratore abilitato, circa tutti gli acquisti "a carattere d'urgenza".

b) Tesoreria

Attività sensibili:

- Autorizzazione degli Ordini di Pagamento.

Processi e ruoli aziendali coinvolti:

- Autorizzazione degli Ordini di Pagamento - Procuratore abilitato.

Controlli esistenti:

Per ciò che concerne la presente Area a Rischio e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Segregazione delle funzioni tra chi predispone gli ordini di pagamento e chi li approva;
- Autorizzazione degli ordini di pagamento da parte del procuratore abilitato, nel rispetto delle procure in essere;
- Verifica della corrispondenza tra fattura e ordine/contratto;
- Verifica, da parte del procuratore abilitato, precedentemente al rilascio dell'autorizzazione al pagamento, dei seguenti aspetti:
    - completa ed accurata compilazione della proposta di pagamento;
    - presenza di una fattura autorizzata (presenza del benestare al pagamento della fattura);
    - corrispondenza tra il beneficiario indicato nella proposta di pagamento e il fornitore indicato in fattura;
    - corrispondenza tra l'importo della proposta di pagamento e quello indicato in fattura.

Reati astrattamente ipotizzabili ed esemplificazioni delle modalità di commissione dei reati nell'ambito delle Aree potenzialmente a Rischio Reato

- False comunicazioni sociali (artt. 2621 c.c.);
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Illecita influenza sull'Assemblea (art. 2636 c.c.).

I reati di false comunicazioni sociali e di false comunicazioni sociali in danno della società, dei soci e dei creditori potrebbero potenzialmente configurarsi nel caso di realizzazione di una delle seguenti condotte indicate a mero titolo esemplificativo e non esaustivo:

- determinazione di poste valutative di bilancio non conformi alla reale situazione economica, patrimoniale e finanziaria di Teleippica, come risulterebbe dalla corretta applicazione dei principi contabili di riferimento, in collaborazione con gli amministratori, anche in concorso con altri soggetti;
- esposizione in bilancio di altre poste (non valutative) inesistenti o di valore difforme da quello reale, ovvero occultamento di fatti rilevanti tali da mutare la rappresentazione delle effettive condizioni economiche della Società, con conseguente pregiudizio della corretta rappresentazione del bilancio d'esercizio (ad esempio, sovrastima o sottostima delle immobilizzazioni materiali, immateriali o finanziarie; falsa rilevazione del valore di ammortamento di alcuni beni, ecc.);
- modifica o alterazione dei dati contabili presenti sul sistema informatico, al fine di dare una rappresentazione della situazione patrimoniale, economica e finanziaria della Società difforme dal vero, anche in concorso con altri soggetti.

Il reato di impedito controllo potrebbe potenzialmente configurarsi nel caso di scarsa o mancata trasparenza e correttezza nella condotta degli amministratori o dei loro diretti collaboratori, in relazione alla richiesta di informazioni da parte dei soci e/o del Collegio Sindacale, attuata mediante l'occultamento di documenti e/o l'esibizione parziale o alterata della documentazione richiesta, anche accompagnata da artifici.

Il reato di indebita restituzione dei conferimenti potrebbe potenzialmente configurarsi nel caso di realizzazione di una delle seguenti condotte, indicate a mero titolo esemplificativo e non esaustivo:

- restituzione dei conferimenti al di fuori delle ipotesi di legittima riduzione del capitale sociale;
- liberazione dall'obbligo di eseguire i conferimenti, attuata anche mediante la falsificazione, l'alterazione o la distruzione dei documenti di rendicontazione.

Il reato di illegale ripartizione degli utili e delle riserve potrebbe potenzialmente configurarsi nel caso di realizzazione di una delle seguenti condotte, indicate a mero titolo esemplificativo e non esaustivo:

- ripartizione di utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, attuata anche mediante la falsificazione, l'alterazione o la distruzione dei documenti di rendicontazione;
- ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite, anche mediante la falsificazione, l'alterazione o la distruzione dei documenti di rendicontazione.

Il reato di operazioni in pregiudizio dei creditori potrebbe potenzialmente configurarsi nel caso di realizzazione di una delle seguenti condotte, indicate a mero titolo esemplificativo e non esaustivo:

- determinazione di poste valutative di bilancio non conformi alla reale situazione economica, patrimoniale e finanziaria della Società, ovvero esposizione in bilancio di altre poste (anche non valutative) inesistenti o di valore difforme da quello reale;
- determinazione di poste valutative di bilancio non conformi alla reale situazione economica, patrimoniale e finanziaria della Società, come risulterebbe dalla corretta applicazione dei principi contabili di riferimento, in collaborazione con gli amministratori;
- occultamento di fatti rilevanti tali da mutare la rappresentazione delle effettive condizioni economiche della Società, anche in concorso con altri soggetti;
- esposizione di dati idonei a pregiudicare i diritti dei creditori sociali in occasione di fusioni/scissioni o riduzioni di capitale;
- adozione di procedure, in occasione di fusioni, scissioni, riduzioni di capitale e altre operazioni straordinarie, che violano i diritti previsti dalla legge a favore dei creditori sociali in relazione a tali operazioni (ad esempio, diritto di opposizione);
- modifica o alterazione dei dati contabili presenti sul sistema informatico, al fine di dare una rappresentazione della situazione patrimoniale, economica e finanziaria della Società difforme dal vero;
- riduzione del capitale sociale al di fuori delle ipotesi legislativamente consentite o al disotto del limite legale (pari ad Euro 10.000 per le società a responsabilità limitata).

Il reato di formazione fittizia del capitale potrebbe potenzialmente configurarsi nel caso di realizzazione delle seguenti condotte, indicate a mero titolo esemplificativo e non esaustivo:

- sopravvalutazione dei beni posseduti, al fine di fornire all'esterno la rappresentazione di una solida situazione patrimoniale della Società, nel concreto non corrispondente alla realtà;
- formazione o aumento fittizio del capitale sociale, mediante attribuzione di quote sociali per un valore complessivamente superiore all'effettivo ammontare del capitale sociale.

Il reato di illecita influenza sull'assemblea potrebbe potenzialmente configurarsi nel caso di realizzazione della seguente condotta, indicata a mero titolo esemplificativo e non esaustivo:

- simulazione o fraudolenta predisposizione o rappresentazione di atti non veritieri e corretti da sottoporre all'approvazione dell'assemblea, al fine di creare un falso convincimento su specifiche circostanze ed ottenere il consenso della maggioranza dei soci, che in conseguenza di tali condotte ingannatorie, non si sarebbe formato.

4.2. Le Aree potenzialmente a Rischio Reato totalmente o parzialmente esternalizzate

Di seguito è riportato l'elenco delle Aree potenzialmente a Rischio Reato, o porzioni di esse, e delle relative attività "sensibili" esternalizzate ad altre società, anche facenti parte del Gruppo Snai.

a) Acquisto di beni e servizi

Attività sensibili:

- Rilevazione del fabbisogno di beni e/o servizi ed emissione della richiesta di acquisto;
- Selezione del fornitore;
- Ricezione beni e servizi;
- Selezione dei consulenti;
- Definizione e monitoraggio degli onorari dei consulenti.

b) Amministrazione, contabilità e bilancio

Attività sensibili:

- Gestione della Contabilità Clienti: Gestione dell'anagrafica dei clienti ed emissione delle fatture attive;
- Gestione della Contabilità Fornitori: Gestione dell'anagrafica fornitori, registrazione e contabilizzazione della fatture passive;
- Tenuta delle scritture obbligatorie e dei Libri (IVA, Libro cespiti, Inventari, ecc.);
- Gestione delle attività propedeutiche alla predisposizione del Bilancio (scritture di rettifica e chiusura) e delle situazioni infrannuali;
- Predisposizione delle situazioni infrannuali;
- Predisposizione del Bilancio Annuale;
- Collaborazione con gli Organi di Controllo (Collegio Sindacale, Società di Revisione, ecc.).

c) Tesoreria

Attività sensibili:

- Gestione degli incassi e dei pagamenti;
- Gestione dei conti correnti bancari e/o postali;
- Gestione delle riconciliazioni bancarie;
- Coordinamento della pianificazione finanziaria di Teleippica con quella della Capogruppo Snai;
- Gestione dei rapporti con gli istituti di credito e finanziari per la negoziazione delle condizioni di accesso al credito e delle relative forme di garanzia;
- Gestione di operazioni finanziarie di straordinaria amministrazione.

Controlli preventivi applicabili a tutte le Aree potenzialmente a Rischio Reato totalmente o parzialmente esternalizzate:

- formale definizione della politica per la esternalizzazione delle attività della Società, anche mediante individuazione dei metodi per la valutazione del livello delle prestazioni del fornitore (S.L.A.);
- formalizzazione di contratti di outsourcing nell'ambito dei quali è prevista:

  - l'identificazione dei servizi da erogare ed il relativo livello di servizio atteso (S.L.A.);
  - l'inserimento di clausole specifiche nell'ambito delle quali la società mandataria si impegna a rispettare i presidi di controllo previsti nel proprio Modello (ove adottato dalla società mandataria) nonché i principi ispiratori del Modello di Teleippica;
  - l'inserimento di clausole specifiche nell'ambito delle quali le società si impegnano, nei confronti l'una dell'altra, al rispetto più rigoroso dei propri Modelli (ove adottati), con particolare riguardo alle aree dei Modelli che presentano rilevanza ai fini delle attività gestite mediante contratto di *outsourcing* e della sua esecuzione; con tali clausole, si impegnano altresì a darsi reciprocamente notizia di eventuali violazioni, che dovessero verificarsi e che possano avere attinenza con il contratto e/o la sua esecuzione e più in generale, ad astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che possano integrare una qualsivoglia fattispecie di reato contemplata dal Decreto;
  - l'applicazione di sanzioni (ivi inclusa l'eventuale risoluzione del contratto) in caso di violazioni alle suddette prescrizioni.

5. Principi e regole di comportamento

E' fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato previste dall'articolo 25-*ter* del D.Lgs. 231/2001.
La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei Destinatari di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.

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

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi, o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria delle Società;
- omettere la comunicazione di dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- alterare i dati e le informazioni destinati alla predisposizione del prospetto di bilancio;
- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- distribuire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- formare o aumentare fittiziamente il capitale sociale, attribuendo quote per valore inferiore al loro valore nominale in sede di costituzione della società o di aumento del capitale sociale;
- distrarre i beni sociali, in sede di liquidazione della società, dalla loro destinazione ai creditori, ripartendoli tra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli;
- illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento dell'attività di controllo da parte del Collegio Sindacale o di altri organi sociali dotati di poteri ispettivi;

- 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;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti, in relazione alle condizioni economiche, patrimoniali o finanziarie della Società.

Al fine di assicurare l'adeguata tracciabilità dei processi operativi e decisionali nell'ambito delle Aree a Rischio precedentemente indicate, tutti i Soggetti Apicali e/o Sottoposti, sono tenuti ad assicurare un'adeguata ricostruibilità *ex post* di ogni operazione effettuata.

Tutti i Soggetti Apicali e/o Sottoposti sono tenuti ad agire nel pieno rispetto del sistema di deleghe e poteri adottato dalla Società.

Il sistema di attribuzione dei compiti della Società è improntato al principio di segregazione dei poteri, in forza del quale ogni processo operativo o decisionale nell'ambito delle Aree a Rischio precedentemente indicate è posto in essere mediante la condivisione delle specifiche attività tra più soggetti, secondo le rispettive competenze.

Segnatamente per ogni operazione contabile deve essere conservata agli atti sociali una adeguata documentazione di supporto dell' attività svolta, in modo da consentire:
a) l'agevole registrazione contabile;
b) l'individuazione dei diversi livelli di responsabilità;
c) la ricostruzione accurata della operazione, anche al fine di ridurre la probabilità di errori interpretativi.

Il sistema di controllo di Teleippica è costituito nelle sue linee generali secondo i principi di controllo generali, di seguito descritti:

TRACCIABILITA' DELLE OPERAZIONI/ATTI

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

SEGREGAZIONE DELLE FUNZIONI

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

IDENTIFICAZIONE E RESPONSABILITA' DELL' OPERAZIONE /PROCESSO

La responsabilità di una operazione/processo aziendale è chiaramente e formalmente definita e diffusa all'interno dell'organizzazione.

LE FALSE COMUNICAZIONI SOCIALI

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

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

Tali situazioni devono, in ogni caso, essere tempestivamente comunicate all'OdV;

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

LA TUTELA DEI CREDITORI E DEL CAPITALE SOCIALE

Per la prevenzione dei reati relativi alle operazioni in pregiudizio dei creditori attraverso la riduzione del capitale sociale o fusioni con altra società o scissioni cagionando danno ai creditori e per i reati relativi alla gestione delle operazioni concernenti conferimenti, distribuzione di utili o riserve, sottoscrizione ed acquisto di azioni o quote sociali, operazioni sul capitale, fusioni e scissioni, è necessario che le attività svolte in azienda garantiscano:

- l'esplicita approvazione, da parte del Consiglio di Amministrazione, di ogni attività relativa alla costituzione di nuove società, all'acquisizione o alienazione di partecipazioni societarie, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni;
- l'espletamento di apposite riunioni tra il Collegio Sindacale e l'OdV.

6. Compiti dell'OdV

Fermi restando i compiti e le funzioni dell'Organismo di Vigilanza statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati Societari lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei Reati Societari previsti dal Decreto;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV svolge in piena autonomia le proprie attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici e/o a campione sulle attività connesse ai Reati Societari, al fine di verificare la corretta implementazione delle stesse in relazione alle regole previste nel Modello. A tal fine, all'OdV, viene garantito libero accesso a tutta la documentazione aziendale rilevante.

L'OdV comunica i risultati della propria attività di controllo relativamente ai Reati Societari al Consiglio di Amministrazione e al Collegio Sindacale secondo quanto previsto nella Parte Generale del Modello.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale B1

Corruzione tra privati
(Art. 25-ter D. Lgs 231/2001)

TELEIPPICA SRL

INDICE

1. Premessa

La legge del 6 novembre 2012, n. 190, adeguando il nostro ordinamento ad una serie di obblighi internazionali e nell'ambito di una più ampia riforma dei delitti di corruzione previsti dal codice penale e da altre disposizioni normative, ha introdotto nel novero dei reati presupposto della responsabilità dell'Ente il delitto di **Corruzione tra privati** di cui all'art. 2635 c.c.
La presente Parte Speciale concerne, in particolare, i comportamenti che devono essere tenuti dai soggetti – Amministratori, dirigenti e dipendenti di Teleippica S.r.l. (di seguito "*Teleippica*" o "*Società*"), anche per il tramite di fornitori e consulenti che svolgono la propria prestazione all'interno della Società, indipendentemente dalla qualificazione giuridica del loro rapporto con la Società - che sono coinvolti nei processi e nelle attività sensibili ed operano pertanto nelle Aree a Rischio Reato (qui di seguito i "Destinatari").
Tutti i Destinatari della presente Parte Speciale del Modello sono tenuti ad adottare comportamenti conformi a quanto di seguito formulato, al fine di prevenire la commissione del reato in oggetto.

2. Il reato di corruzione tra privati di cui all'art. 25-ter del D.Lgs. 231/2001 – Esempi delle modalità di commissione

Viene riportato di seguito il testo dell'art. 2635 c.c., unitamente ad un breve commento della fattispecie.

- **Corruzione tra privati (art. 2635 c.c.)**

"Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.
Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.
Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.
Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.
Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi."

All'interno dell'art. 25-*ter* del D.Lgs. 231/01 è stato, tuttavia, recepito solo il terzo comma, che punisce la dazione (indebita) di denaro o altra utilità.
Il reato si potrebbe pertanto configurare attraverso la dazione o la promessa di denaro o altra utilità (per sé o per altri) ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori al fine che essi compiano od omettano atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società di appartenenza.
Nell'ambito della responsabilità dell'Ente deve altresì configurarsi il vantaggio o l'interesse dell'ente stesso, connesso al nocumento cagionato dal soggetto corrotto alla sua società.

3. Le sanzioni previste in relazione al delitto di corruzione tra privati di cui all'art 25-ter del D.Lgs. 231/2001

Si riporta, di seguito, la sanzione prevista in relazione al delitto di corruzione tra privati, qualora, per effetto della commissione dello stesso, da parte dei soggetti apicali e/o dei soggetti sottoposti, derivi all'Ente un interesse o un vantaggio.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
Corruzione tra privati (art. 2635 c.c.)	Da 200 a 400 quote	Nessuna

4. Le aree a potenziale rischio reato diretto e le aree c.d. "strumentali"

Nel corso dell'attività di analisi condotta nell'ambito delle varie Direzioni/Funzioni aziendali, Teleippica ha provveduto ad individuare le aree a rischio reato costituite da:

- aree a rischio "***reato diretto***", ossia nel cui ambito sono poste in essere attività, che per effetto di contatti diretti con i soggetti indicati nel primo comma dell'art. 2635 c.c., comportino il rischio diretto di commissione del reato (qui di seguito "***Aree a Rischio Reato Diretto***");
- aree a rischio c.d. "***strumentali***" alla realizzazione del reato, ossia aree che, essendo connesse alla gestione di strumenti di tipo finanziario, possono supportare la commissione del reato attraverso la creazione di provviste (qui di seguito "***Aree a Rischio Reato Strumentali***").

Si riporta, di seguito, l'indicazione delle Aree a Rischio individuate dalla Società in relazione al reato di corruzione tra privati:

Aree a Rischio Reato Diretto:

- Gestione dei rapporti con enti certificatori di natura privata;
- Gestione del contenzioso;
- Acquisto di beni e servizi;
- Gestione dei contenuti editoriali;
- Gestione della comunicazione e dei rapporti con i media.

Aree a Rischio Reato Strumentali:

- Selezione ed assunzione del personale;
- Amministrazione del personale*;*
- Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza;
- Amministrazione, contabilità e bilancio;
- Tesoreria.

Nell'ambito di ciascuna **Area a Rischio Reato Diretto o Strumentale, gestita totalmente o parzialmente da Teleippica**, sono state individuate le c.d. "attività sensibili", ossia quelle attività al cui svolgimento è connesso il rischio di commissione del reato di corruzione tra privati.
Sono state, inoltre, identificate le funzioni o i ruoli aziendali coinvolti nell'esecuzione di tali attività "sensibili". L'individuazione dei ruoli/funzioni non deve considerarsi, in ogni caso, tassativa atteso che ciascun soggetto aziendale potrebbe in linea teorica essere coinvolto.
Sono stati individuati, altresì, in via esemplificativa, con riferimento a ciascuna area, alcune potenziali modalità di realizzazione dei reati ed i principali controlli previsti con riferimento alle attività poste in essere nelle Aree a Rischio.

Invece, nell'ambito di ciascuna **Area a Rischio Reato Diretto o Strumentale, esternalizzata ad altre società**, anche facenti parte del Gruppo Snai, sono state individuate le relative attività "sensibili" e i principali controlli preventivi posti in essere in relazione alle aree "a rischio", o porzioni di esse, esternalizzate.

Di seguito è riepilogato il quadro in precedenza esposto.

4.1. Le Aree potenzialmente a Rischio Reato Diretto gestite parzialmente o totalmente da Teleippica. Le attività "sensibili", i ruoli aziendali coinvolti, le potenziali modalità di realizzazione dei reati ed i presidi di controllo esistenti

a) Gestione dei rapporti con enti certificatori di natura privata

Attività sensibili:

- Predisposizione e trasmissione di informazioni ad enti certificatori di natura privata;
- Gestione dei rapporti con enti certificatori privati nell'ambito di attività ispettive, finalizzate al rilascio o rinnovo della certificazione.

Processi e ruoli aziendali coinvolti:

- Gestione dei rapporti con enti certificatori privati – Responsabile Funzione Service Management / Responsabile Funzione Esercizio/ Responsabile Funzione Produzione/ Responsabile Funzione Progettazione e Post Produzione/ Responsabile Funzione Rete.
-

Esemplificazioni delle modalità di commissione del reato di corruzione tra privati:

- La Società potrebbe trasmettere ad enti certificatori di natura privata documentazione non veritiera o alterata, anche in relazione alla richiesta di informazioni o chiarimenti, con la finalità di condizionare il rilascio o il rinnovo della certificazione o potrebbe offrire o promettere utilità ad un esponente di un organismo di certificazione di natura privata che, agendo in violazione degli obblighi inerenti al proprio ufficio, in sede di rilascio o rinnovo della certificazione, ovvero in sede di verifica, attesta falsamente il rispetto delle norme di riferimento.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Diretto e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Identificazione dei soggetti autorizzati ad intrattenere rapporti con gli enti certificatori per la richiesta, l'ottenimento e la gestione delle certificazioni;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei rapporti con enti certificatori di natura privata;
- Rispetto del principio di segregazione tra chi predispone la documentazione da trasmettere agli enti certificatori e chi la verifica;
- Verifica della completezza ed accuratezza dei documenti da inviare agli enti certificatori ai fini dell'ottenimento e la gestione delle certificazioni;

- Sistematico monitoraggio della sussistenza di tutti i requisiti necessari per accedere alla certificazione;
- Sistematico monitoraggio delle scadenze delle certificazioni e dei termini di rinnovo;
- Formalizzazione di quanto comunicato e trasmesso all'ente certificatore competente nell'ambito di eventuali visite ispettive.

b) Gestione del contenzioso

Attività sensibili:

- Definizione ed autorizzazione delle strategie societarie in relazione alla gestione dei contenziosi;
- Definizione ed autorizzazione di accordi transattivi;
- Sottoscrizione di atti, adempimenti e dichiarazioni relativamente ai contenziosi e/o agli accordi transattivi in essere (Fiscali, amministrativi, civili, giuslavoristici, ecc.).

Processi e ruoli aziendali coinvolti:

- Definizione ed autorizzazione delle strategie societarie in relazione alla gestione dei contenziosi e degli accordi transattivi - Amministratore Delegato / Consiglio di Amministrazione.

Esemplificazioni delle modalità di commissione del reato di corruzione tra privati:

- La Società, al fine di garantirsi un esito positivo della contesa o un accordo transattivo particolarmente vantaggioso, con nocumento per la società controparte nel procedimento, potrebbe, anche attraverso i legali esterni, offrire o promettere denaro o altre utilità ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari o sindaci della controparte ovvero a persone o società a questi direttamente o indirettamente collegate.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Diretto e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Individuazione dei soggetti autorizzati a rappresentare la Società nel corso di contenziosi e accordi transattivi (es. fiscali, amministrativi, civili, giuslavoristici, ecc.).
- Sistematico coinvolgimento del vertice aziendale in merito alla definizione delle linee guida da seguire per la gestione delle controversie e/o per la definizione di accordi transattivi;
- Formale autorizzazione delle strategie societarie in relazione alla gestione dei contenziosi e degli accordi transattivi;
- Informativa regolare e periodica verso il vertice aziendale in merito ai contenziosi in essere.

c) Acquisto di beni e servizi

Attività sensibili:

- Autorizzazione degli ordini di acquisto;
- Emissione del benestare al pagamento.

Processi e ruoli aziendali coinvolti:

- Autorizzazione degli approvvigionamenti sulla base del sistema di deleghe e procure vigente – Responsabile Area Richiedente/ Procuratori abilitato.
- Emissione del benestare al pagamento – Tutti i referenti interessati.

Esemplificazioni delle modalità di commissione del reato di corruzione tra privati:

- La Società potrebbe corrompere un esponente di una società fornitrice al fine di ottenere condizioni più vantaggiose nella fornitura, con conseguente nocumento della Società fornitrice. L'area in oggetto, inoltre, può costituire un mezzo per creare disponibilità extracontabili da utilizzare per attribuire indebiti vantaggi a soggetti privati: si pensi, ad esempio, all'ipotesi della selezione e dell'utilizzo di fornitori fittizi, ovvero alla predisposizione, all'autorizzazione e al benestare di ordini di acquisto anch'essi fittizi, tutte attività potenzialmente finalizzate a disporre di fondi extracontabili da destinare a scopi corruttivi.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Diretto e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Previsione, all'interno del Codice Etico, che tutti i rapporti con terzi siano ispirati a principi di lealtà, correttezza e onestà;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei flussi di approvvigionamento;
- Previsione, all'interno di tutti i contratti stipulati, di clausole di accettazione da parte della controparte, del modello 231 e del Codice Etico di Teleippica;
- Regolamentazione del rapporto con i fornitori tramite appositi contratti /accordi quadro, autorizzati nel rispetto delle procure esistenti;
- Approvazione dei contratti di approvvigionamento secondo i livelli autorizzativi definiti dalla Società in base agli importi degli stessi;
- Segregazione di funzioni tra chi attesta la ricezione del bene/servizio e approva la fattura e chi effettua/autorizza il pagamento;
- Monitoraggio delle prestazioni ricevute tramite verifica dell'allineamento con quanto concordato a livello contrattuale;
- Verifica della ricezione dei beni e servizi e del rispetto delle relative condizioni contrattuali prima di fornire il benestare al pagamento;
- Formale autorizzazione degli acquisti in "extra-budget";

- Formale identificazione delle modalità di gestione degli acquisti "a carattere d'urgenza";
- Verifica a posteriori, da parte del procuratore abilitato, circa tutti gli acquisti "a carattere d'urgenza".

d) Gestione dei contenuti editoriali

Attività sensibili:

- Definizione e approvazione del contratto giornalistico e del prezzo finale di acquisto del servizio;
- Monitoraggio degli adempimenti contrattuali.

Processi e ruoli aziendali coinvolti:

- Gestione dei servizi giornalistici – Area Editoriale.

Esemplificazioni delle modalità di commissione del reato di corruzione tra privati:

- La Società potrebbe corrompere un esponente di una società fornitrice al fine di ottenere condizioni più vantaggiose nella fornitura, con conseguente nocumento della Società fornitrice. L'area in oggetto, inoltre, può costituire un mezzo per creare disponibilità extracontabili da utilizzare per attribuire indebiti vantaggi a soggetti privati: si pensi, ad esempio, all'ipotesi della selezione e dell'utilizzo di giornalisti fittizi, ovvero alla predisposizione, all'autorizzazione e al benestare di ordini di acquisto anch'essi fittizi, tutte attività potenzialmente finalizzate a disporre di fondi extracontabili da destinare a scopi corruttivi.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Diretto e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Previsione, all'interno del Codice Etico, che tutti i rapporti con le Terze Parti siano ispirati a principi di lealtà, correttezza e onestà;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei contenuti editoriali ed, in particolare, l'acquisizione di servizi giornalistici;
- Previsione, all'interno di tutti i contratti stipulati, di clausole di accettazione, da parte della controparte, del Modello 231 e del Codice Etico di Teleippica;
- Segregazione delle funzioni tra chi definisce gli importi dei contratti e chi approva i contratti editoriali, con particolare riferimento ai servizi giornalistici;
- Autorizzazione dei contratti editoriali, ed in particolare di quelli giornalistici, da parte del procuratore abilitato, nel rispetto delle procure in essere;
- Verifica degli adempimenti, degli obblighi e delle condizioni contrattuali posti in capo ai consulenti esterni (es. giornalisti, ecc.).

e) Gestione della comunicazione e dei rapporti con i mass media

Attività sensibili:

- Comunicazione esterna e gestione dei rapporti con i mass media (comunicazioni sulla società o comunicazioni di prodotto / servizio).

Processi e ruoli aziendali coinvolti:

- Comunicazione esterna e gestione dei rapporti con i mass media – Area Editoriale.

Esemplificazioni delle modalità di commissione del reato di corruzione tra privati:

- La Società, interessata ad ottimizzare il proprio posizionamento strategico e promuovere la propria immagine, ovvero ad occultare o edulcorare la modalità di diffusione di notizie negative sul proprio conto, potrebbe corrompere, per il tramite di propri apicali o sottoposti, esponenti dei media (es. stampa o televisione) attraverso indebite promesse di denaro o di future utilità o favori di vario genere.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Diretto e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Identificazione dei soggetti delegati a gestire le comunicazioni verso l'esterno ed i rapporti con i mass media;
- Integrità, imparzialità e indipendenza, non influenzando impropriamente le decisioni dei media e non richiedendo trattamenti di favore;
- Divieto di diffondere informazioni a media che siano fuorvianti o non rispondenti al vero, mascherando, ad esempio, una situazione di dissesto della Società;
- Verifica preventiva di completezza, accuratezza e veridicità di tutte le informazioni ed i dati trasmessi ai mass media;
- Sistematico coinvolgimento dell'Amministratore Delegato nella definizione preventiva di qualsiasi comunicazione, al fine di prevenire il rischio di diffusione di notizie false o fuorvianti riguardanti le condizioni della Società.

4.2. Le Aree potenzialmente a Rischio Reato Strumentali gestite parzialmente o totalmente da Teleippica. Le attività "sensibili", i ruoli aziendali coinvolti ed i presidi di controllo esistenti

a) Selezione ed assunzione del personale

Attività sensibili:

- Assunzione del candidato.

Processi e ruoli aziendali coinvolti:

- Gestione delle attività connesse all'assunzione del personale - Amministratore Delegato / Consiglio di Amministrazione.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Definizione delle responsabilità e dei livelli autorizzativi nell'ambito del processo di assunzione;
- Formalizzazione del contratto di assunzione e autorizzazione dello stesso secondo i suddetti livelli autorizzativi;
- Regolamentazione, all'interno del contratto di assunzione, della retribuzione spettante al neoassunto, dell'eventuale previsione di premi di produttività o altri elementi di retribuzione variabile, nonché dell'utilizzo di eventuali benefit aziendali;
- Previsione, all'interno del contratto di assunzione, delle clausole di accettazione del Modello 231 e del Codice Etico di Teleippica;
- Autorizzazione, da parte del procuratore abilitato, di qualsiasi modifica alle condizioni contrattuali non derivante dalla contrattazione collettiva.

b) Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza

Attività sensibili:

- Definizione ed approvazione delle iniziative legate all'omaggistica;
- Gestione delle ospitalità e delle spese di rappresentanza.

Processi e ruoli aziendali coinvolti:

- Definizione ed approvazione delle iniziative legate all'omaggistica – Amministratore Delegato;
- Gestione delle ospitalità e delle spese di rappresentanza – Procuratore Abilitato.

Presidi di controllo esistenti:
Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.
In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dell'omaggistica, delle ospitalità e delle spese di rappresentanza;
- Previsione ed autorizzazione, in base alle deleghe vigenti, di un budget degli omaggi, delle ospitalità e delle spese di rappresentanza;
- Previsione, all'interno dei contratti, delle clausole di accettazione del Modello 231 e del Codice Etico di Teleippica da parte della controparte;
- Formale identificazione dei soggetti responsabili all'autorizzazione degli omaggi;
- Autorizzazione preventiva ai fini della concessione di ospitalità e spese di rappresentanza;
- Verifica delle spese di rappresentanza ed ospitalità sostenute e sottoposizione delle stesse a specifica autorizzazione da parte del Procuratore Abilitato.

e) Tesoreria

Attività sensibili:

- Autorizzazione degli Ordini di Pagamento;
- Gestione della piccola cassa.

Processi e ruoli aziendali coinvolti:

- Autorizzazione degli ordini di pagamento - Procuratore abilitato.
- Gestione della piccola cassa.

Controlli esistenti:
Per ciò che concerne la presente Area a Rischio Strumentale e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.
In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Segregazione delle funzioni tra chi predispone gli ordini di pagamento e chi li approva;
- Autorizzazione degli ordini di pagamento da parte del procuratore abilitato, nel rispetto delle procure in essere;
- Verifica della corrispondenza tra fattura e ordine/contratto;
- Verifica, da parte del procuratore abilitato, precedentemente al rilascio dell'autorizzazione al pagamento, dei seguenti aspetti:
  - completa ed accurata compilazione della proposta di pagamento;

  - presenza di una fattura autorizzata (presenza del benestare al pagamento della fattura);
  - corrispondenza tra il beneficiario indicato nella proposta di pagamento e il fornitore indicato in fattura;
  - corrispondenza tra l'importo della proposta di pagamento e quello indicato in fattura;
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione della piccola cassa;
- Definizione del limite di importo massimo della piccola cassa (giacenza massima);
- Definizione delle tipologie di spese che possono essere sostenute tramite cassa, del relativo ammontare massimo e dei soggetti abilitati ad autorizzarle;
- Verifica di corrispondenza tra le spese autorizzate ed i relativi giustificativi di spesa;
- Definizione delle modalità operative di reintegro della piccola cassa;
- Riconciliazione periodica, fisico-contabile, dei valori di cassa.

4.3. Le Aree potenzialmente a Rischio Reato Diretto o Strumentali totalmente o parzialmente esternalizzate

Di seguito è riportato l'elenco delle Aree potenzialmente a Rischio Reato Diretto o Strumentali, o porzioni di esse, e delle relative attività "sensibili" esternalizzate ad altre società, anche facenti parte del Gruppo Snai.

a) Gestione del contenzioso

Attività sensibili:
- Supporto nella gestione dei contenziosi e degli accordi transattivi (fiscali, amministrativi, civili, giuslavoristici, ecc.);
- Selezione dei consulenti legali esterni;
- Monitoraggio sugli onorari e sull'attività svolta dai consulenti legali esterni.

b) Acquisto di beni e servizi

Attività sensibili:
- Rilevazione del fabbisogno di beni e/o servizi ed emissione della richiesta di acquisto;
- Selezione del fornitore;
- Ricezione beni e servizi;
- Selezione dei consulenti;
- Definizione e monitoraggio degli onorari dei consulenti.

c) Selezione ed assunzione del personale

Attività sensibili:
- Definizione dei criteri di selezione del personale in relazione al profilo ricercato;
- Selezione del personale.

d) Amministrazione del personale

Attività sensibili:

- Gestione dell'anagrafica dipendenti;
- Rilevazione delle presenze;
- Elaborazione dei cedolini del personale dipendente e parasubordinato;
- Gestione note spese e trasferte.

e) Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza

Attività sensibili:

- Gestione delle iniziative legate all'omaggistica.

f) Gestione contenuti editoriali

Attività sensibili:

- Selezione dei consulenti (giornalisti);
- Definizione e monitoraggio degli onorari dei consulenti.

g) Amministrazione, contabilità e bilancio

Attività sensibili:

- Gestione della Contabilità Clienti: Gestione dell'anagrafica dei clienti ed emissione delle fatture attive;
- Gestione della Contabilità Fornitori: Registrazione e contabilizzazione della fatture passive,
- Tenuta delle scritture obbligatorie e dei Libri (IVA, Libro cespiti, Inventari, ecc.);
- Gestione delle attività propedeutiche alla predisposizione del Bilancio (scritture di rettifica e chiusura) e delle situazioni infrannuali;
- Predisposizione delle situazioni infrannuali;
- Predisposizione del Bilancio Annuale;
- Collaborazione con gli Organi di Controllo (Collegio Sindacale, Società di Revisione, ecc.).

h) Tesoreria

Attività sensibili:

- Gestione degli incassi e dei pagamenti;
- Gestione dei conti correnti bancari e/o postali;
- Gestione delle riconciliazioni bancarie;
- Coordinamento della pianificazione finanziaria di Teleippica con quella della Capogruppo Snai;

- Gestione dei rapporti con gli istituti di credito e finanziari per la negoziazione delle condizioni di accesso al credito e delle relative forme di garanzia;
- Gestione di operazioni finanziarie di straordinaria amministrazione.

Controlli preventivi applicabili a tutte le Aree potenzialmente a Rischio Reato Diretto o Strumentali totalmente o parzialmente esternalizzate:

- formale definizione della politica per la esternalizzazione delle attività della Società, anche mediante individuazione dei metodi per la valutazione del livello delle prestazioni del fornitore (S.L.A.);
- formalizzazione di contratti di outsourcing nell'ambito dei quali è prevista:
  - l'identificazione dei servizi da erogare ed il relativo livello di servizio atteso (S.L.A.);
  - l'inserimento di clausole specifiche nell'ambito delle quali la società mandataria si impegna a rispettare i presidi di controllo previsti nel proprio Modello (ove adottato dalla società mandataria) nonché i principi ispiratori del Modello di Teleippica;
  - l'inserimento di clausole specifiche nell'ambito delle quali le società si impegnano, nei confronti l'una dell'altra, al rispetto più rigoroso dei propri Modelli (ove adottati), con particolare riguardo alle aree dei Modelli che presentano rilevanza ai fini delle attività gestite mediante contratto di outsourcing e della sua esecuzione; con tali clausole, si impegnano altresì a darsi reciprocamente notizia di eventuali violazioni, che dovessero verificarsi e che possano avere attinenza con il contratto e/o la sua esecuzione e più in generale, ad astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che possano integrare una qualsivoglia fattispecie di reato contemplata dal Decreto;
  - l'applicazione di sanzioni (ivi inclusa l'eventuale risoluzione del contratto) in caso di violazioni alle suddette prescrizioni.

5. Principi e regole di comportamento

E' fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di reato in oggetto.
La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei Destinatari di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutti i rapporti (contrattuali e non) con soggetti di entità terze;
- adottare un comportamento improntato ai principi di integrità, onestà e buona fede in relazione ai rapporti con i terzi;
- definire per iscritto qualsiasi tipo di accordo con consulenti e collaboratori in modo da rendere evidenti i termini dell'accordo stesso – con particolare riguardo alla tipologia di incarico/transazione e alle condizioni economiche sottostanti;
- riferire prontamente all'OdV eventuali situazioni di irregolarità.

Nell'ambito dei suddetti comportamenti, in particolare, sono espressamente vietati:

- la ricerca e l'instaurazione di relazioni personali di favore, l'impropria influenza e l'indebita ingerenza idonee a condizionare, direttamente o indirettamente, le decisioni della controparte e/o lo svolgimento di un corretto rapporto;
- le offerte o le promesse di denaro o di beni o di altre utilità (in qualunque forma e modo) a amministratori, dirigenti, sindaci o dipendenti di società terze, o a loro parenti, anche in modo indiretto e/o per interposta persona, salvo che si tratti di doni o di beni o di altre utilità di modico valore e siano di natura appropriata, conformi agli usi vigenti nel particolare contesto normativo e sociale ed alle applicabili leggi e sempre che tali doni, beni od altre utilità non possano essere intesi od interpretati come rivolti alla ricerca di favori;
- i pagamenti illeciti, fatti direttamente da società fornitrici/clienti o tramite persone che agiscono per conto di tali enti, sia in Italia che all'estero;
- la valutazione e/o la proposta di opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della controparte a titolo personale nel corso di una trattativa d'affari, richiesta o rapporto commerciale.

Al fine di assicurare l'adeguata tracciabilità dei processi operativi e decisionali nell'ambito delle Aree a Rischio precedentemente indicate, tutti i Soggetti Apicali e/o Sottoposti sono tenuti ad assicurare un'adeguata ricostruibilità *ex post* di ogni operazione effettuata.

Tutti i Soggetti Apicali e/o Sottoposti sono tenuti ad agire nel pieno rispetto del sistema di deleghe e poteri adottato dalla Società.

Il sistema di attribuzione dei compiti della Società è improntato al principio di segregazione dei poteri, in forza del quale ogni processo operativo o decisionale nell'ambito delle Aree a Rischio precedentemente indicate è posto in essere mediante la condivisione delle specifiche attività tra più soggetti, secondo le rispettive competenze.

6. Compiti dell'OdV

Fermi restando i compiti e le funzioni dell'Organismo di Vigilanza statuiti nella Parte Generale del presente Modello, ai fini della prevenzione del reato di corruzione tra privati lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione del reato di corruzione tra privati previsto dal Decreto;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV svolge in piena autonomia le proprie attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici e/o a campione sulle attività connesse al reato di corruzione tra privati, al fine di verificare la corretta implementazione delle stesse in relazione alle regole previste nel Modello. A tal fine, all'OdV, viene garantito libero accesso a tutta la documentazione aziendale rilevante.
L'OdV comunica i risultati della propria attività di controllo al Consiglio di Amministrazione e al Collegio Sindacale secondo quanto previsto nella Parte Generale del Modello.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale C

Reati in materia di salute e sicurezza sul lavoro

(Art. 25-septies D.Lgs. 231/2001)

Teleippica SRL

INDICE

1. Le fattispecie di reato previste dall'art. 25-*septies* del D.Lgs. n. 231/2001

L'art.25-*septies* del D.Lgs. 231/2001 richiama le fattispecie di reato (di seguito per brevità, i "**Reati in materia di salute e sicurezza sul lavoro**") introdotte dall'art. 9 della Legge 3 agosto 2007, n. 123, di omicidio colposo e di lesioni gravi o gravissime derivanti dalla violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

In questa sede è opportuno evidenziare che il TUS ha stabilito un contenuto minimo essenziale del modello organizzativo in questa materia.
L'art. 30 del TUS dispone che:
"Il modello di organizzazione e di gestione idoneo a ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, della società e delle associazioni anche prive di personalità giuridica di cui al D.Lgs. 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- *a) al rispetto degli standard tecnico strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;*
- *b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;*
- *c) alle attività di natura organizzativa, quali emergenze di primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;*
- *d) alle attività di sorveglianza sanitaria;*
- *e) alle attività di informazione e formazione dei lavoratori;*
- *f) alle attività di vigilanza con riferimento al rispetto delle Procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;*
- *g) alle acquisizioni di documentazioni e certificazioni obbligatorie di legge;*
- *h) alle periodiche verifiche dell'applicazione e dell'efficacia delle Procedure adottate.*

Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.
Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.
Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.
Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni ed all'igiene sul lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico".

La norma, pertanto, comporta che per espressa volontà del Legislatore, debbano essere considerate "***a rischio***" e debbano essere presidiate, a prescindere da ogni valutazione di merito sulla concreta possibilità di realizzazione di reati, le aree e le attività indicate ed interessate dall'articolo stesso.

In tema di reati di salute e sicurezza sul lavoro, l'art. 25-*septies* D.Lgs. 231/01, prevede e regolamenta i casi di *"Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro".*

Ai sensi dell'art. 25-*septies* del D.Lgs. 231/01:
"*In relazione al delitto di cui all'art. 589 del codice penale, commesso con violazione dell'art. 55, comma 2, del decreto legislativo attuativo della delega di cui alla l. 3 agosto 2007 n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'art. 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.*
Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'art. 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e della sicurezza sui luoghi di lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'art. 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.
In relazione al delitto di cui all'art. 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro, si applica una sanzione pecuniaria non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'art. 9, comma 2, per una durata non superiore a sei mesi".

Ai sensi dell'art. 55, comma 1 e 2, D.Lgs. 81/2008 8 (TUS):

"*1. E' punito con l'arresto da quattro a otto mesi o con l'ammenda da 2500 a 6400 Euro il Datore di Lavoro:*

a) per la violazione dell'art. 29, comma 1;
b) che non provvede alla nomina del responsabile del servizio prevenzione e protezione ai sensi dell'art. 17, comma 1 lettera b, o per la violazione dell'art. 34, comma 2.
2. Nei casi previsti al comma 1, lettera a), si applica la pena dell'arresto da quattro a otto mesi se la violazione è commessa:
a) Nelle aziende si cui all'art. 31, comma 6 lettera a), b), c) d), f);
b) In aziende che svolgono attività che espongono i lavoratori a rischi biologici di cui all'art. 268, comma 1, lettera c) e d), da atmosfere esplosive, cancerogeni, mutageni e da attività di manutenzione, rimozione, smaltimento e bonifica di amianto;
c) Per le attività disciplinate dal titolo IV caratterizzate dalla compresenza di più imprese e la cui entità presunta di lavoro non sia inferiore a 200, uomini giorno".

Le sanzioni a carico dell'Ente, che operi alle condizioni previste dall'art. 55, comma 2 TUS, sono perciò più severe laddove siano mancate:

- la valutazione dei rischi;
- l'adozione del Documento di Valutazione dei Rischi.

Il reato di omicidio colposo, lesioni colpose gravi e gravissime si configura per il fatto di aver cagionato, per colpa, la morte di un uomo oppure di aver cagionato, per colpa, una lesione personale dalla quale è derivata una malattia grave o gravissima, vale a dire guaribile in più di quaranta giorni (artt. 589 e 590 c.p.).
Il reato costituisce presupposto della responsabilità amministrativa degli enti soltanto se commesso con violazione delle norme sulla prevenzione degli infortuni sul lavoro.
In genere i reati considerati dal D.Lgs. 231/01 sono dolosi, ossia posti in essere volontariamente dal soggetto con quello scopo specifico, e il modello organizzativo ha una funzione di esimente della responsabilità della Società se le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il modello.
I reati considerati in questa Parte Speciale sono, invece, di natura colposa, ossia conseguenza di negligenza, imprudenza, imperizia o inosservanza di leggi e regolamenti da parte dell'autore del reato, e pertanto la funzione di esimente del modello organizzativo, è rappresentata dall'introduzione di previsioni volte a far sì che i Destinatari pongano in essere una condotta (non accompagnata dalla volontà dell'evento morte/lesioni personali) rispettosa delle Procedure previste dal sistema di prevenzione e protezione ai sensi del TUS, congiuntamente agli adempimenti e agli obblighi di vigilanza previsti dal modello organizzativo.
Con riferimento al presupposto per la responsabilità dell'ente, vale a dire l'interesse o il vantaggio derivanti dal reato, occorre osservare che, trattandosi di fatti colposi, non è agevole individuare quale vantaggio o interesse possa derivare ad un ente dal fatto della morte o delle lesioni di un dipendente determinate da colpa.
A tale proposito si tende ad individuare nella condotta, piuttosto che nel reato, i parametri di riferimento per far sorgere la responsabilità dell'ente. Il vantaggio o l'interesse deriverebbero, di conseguenza, non dal fatto della morte o delle lesioni, ma dall'utilità conseguita (ad esempio risparmio in termini di spesa) dalla condotta negligente casualmente correlata all'evento.

I reati considerati nell'art. 25-*septies* del D.Lgs. 231/01 sono qui di seguito riportati:

(i) Omicidio colposo (art. 589 c.p.)

"Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.
Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.
Si applica la pena della reclusione da tre a dieci anni se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale da:
1) soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni;
2) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope
Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici".

(ii) Lesioni personali colpose (art. 590 c.p.)

"Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.
Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239.
Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto è commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni.
Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.
Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale".

2. Le sanzioni previste per i reati in materia di Sicurezza sul lavoro dall'art. 25-*septies* D.Lgs. 231/2001

Si riporta, di seguito, una tabella riepilogativa delle sanzioni previste dall'art. 25-*septies* del D.Lgs. 231/01 a carico della Società, qualora derivi dall'Ente un interesse o un vantaggio, sia pure non direttamente correlato alla commissione della fattispecie di reato individuate dal D.Lgs. 231/01, per le ragioni illustrate nel precedente paragrafo 1.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
• Omicidio colposo (589 del codice penale) con violazione dell'articolo 55, comma 2, del TUS	1000 quote	• Interdizione dall'esercizio dell'attività (da tre mesi a un anno)
• Omicidio colposo (589 del codice penale) con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	Da 250 a 500 quote	• Interdizione dall'esercizio dell'attività (da tre mesi a un anno)
• Lesioni colpose gravi o gravissime (art. 590, 3° comma del codice penale)	Fino a 250 quote	• Interdizione dall'esercizio dell'attività (fino sei mesi)

3. Le aree a Rischio Reato

Al fine di garantire il più elevato grado di sicurezza tecnicamente possibile, le Aree a rischio che Teleippica S.r.l. (di seguito "*Teleippica*" o "*Società*") ha individuato in relazione alla fattispecie di cui all'art. 25- *septies* del D.Lgs. 231/01 si riferiscono alla totalità delle funzioni e delle aree operative della Società.
Nonostante le sostanziali difficoltà di circoscrivere soltanto ad alcune specifiche funzioni o aree operative il rischio di commissione di reati in materia di salute e sicurezza sul lavoro, e quindi di collegare in via generale a singole funzioni/attività aziendali il rischio di commissione degli illeciti considerati dal D.Lgs. 231/2001, l'analisi dell'operatività aziendale ha messo in luce che, tra le attività rilevanti, possono individuarsi le seguenti Aree a rischio reato:

- ***Valutazione delle politiche relative alla Salute e Sicurezza:***
  - Definizione degli obiettivi e dei programmi in materia di Salute e Sicurezza;
  - Applicazione di metodologie di identificazione e valutazione dei rischi;
  - Valutazione dei rischi;
  - Individuazione dei dispositivi di prevenzione individuale;
  - Definizione della politica del riesame ai fini del miglioramento nel tempo dei livelli di sicurezza.

- ***Monitoraggio degli infortuni e degli incidenti:***
  - Analisi del fenomeno infortunistico.
  - Analisi del fenomeno incidentale.

- ***Definizione della struttura organizzativa, individuazione dei ruoli e delle responsabilità in materia di salute e sicurezza.***
  - Gestione del personale in materia di Salute e Sicurezza:
  - Diffusione del sistema sanzionatorio ai dipendenti;
  - Attività di formazione verso il personale.

- ***Sorveglianza Sanitaria:***
  - Predisposizione del Piano di Sorveglianza Sanitaria.

- ***Tracciabilità delle informazioni afferenti a Salute e Sicurezza sul Lavoro:***
  - Archiviazione della documentazione afferente la Salute e la Sicurezza.

- ***Riesame del Sistema di Salute e Sicurezza sul Lavoro:***
  - Monitoraggio continuo sul Sistema di Salute e Sicurezza.

Teleippica ha sede legale in Porcari (LU), Via Luigi Boccherini 39 e sedi operative a Roma (RM), Via Cristoforo Colombo 283/A e Via di Settebagni 384/390, ed occupa circa 60 (sessanta) dipendenti suddivisi in dirigenti, quadri ed impiegati.
In particolare, i dirigenti fanno riferimento al CCNL del l'"*Industria*" mentre, i quadri e gli impiegati, fanno riferimento al CCNL delle "*Imprese Radio Televisive Private*".

I dipendenti di Teleippica svolgono mansioni afferenti: alle riprese televisive, alla definizione e messa in produzione di contenuti editoriali e alle attività di regia relativamente al mondo dell'ippica.
L'attività della Società ha infatti ad oggetto la diffusione delle immagini televisive e multimediali dell'ippica e di tutti gli aspetti di costume legati a tale sport (es. scommesse sulle corse, attività ippica nazionale e internazionale, allevamento e promozione dell'ippica, ecc.).
Inoltre, Teleippica gestisce un canale radio "Radio Snai", la cui programmazione tratta contenuti editoriali, collegamenti e servizi aventi ad oggetto lo sviluppo dell'ippica nazionale ed internazionale.
Nell'ambito delle Aree di Rischio Reato, possono individuarsi, a titolo esemplificativo e non esaustivo, i seguenti adempimenti in materia di salute sicurezza sul luogo di lavoro:

a) Individuazione dei rischi per la salute e la sicurezza sul lavoro;
b) Redazione ed aggiornamento, ai sensi degli artt. 17, 28 e 29 TUS, del Documento di Valutazione del Rischio (di seguito, per brevità "DVR"), con riferimento in particolare a:
    - Analisi di tutti i rischi per la salute e la sicurezza dell'attività lavorativa presenti negli ambienti di lavoro in cui si svolge l'attività di Teleippica e la specificazione dei criteri adottati per la valutazione stessa;
    - Individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione ed addestramento;
    - Individuazione e predisposizione delle misure di prevenzione e protezione e dei dispositivi di protezione individuali e collettivi, idonei ad eliminare i rischi connessi alle attività svolte e quelli presenti sui luoghi di lavoro;
    - Individuazione del programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
    - Individuazione dei ruoli dell'organizzazione aziendale che debbono provvedere all'attuazione delle misure di prevenzione e protezione;
    - Gestione dei rapporti con i Pubblici Ufficiali in caso di visita ispettiva (sul punto si rimanda alla Parte Speciale A relativa ai reati contro la Pubblica Amministrazione);
    - Gestione delle azioni correttive poste in essere a seguito dei rilievi emersi;
    - Rilevazione ed analisi di dati e informazioni con riferimento ai principali eventi in materia di salute e sicurezza sul lavoro;
    - Attività di aggiornamento, formazione ed informazione del personale in materia di salute sicurezza sul lavoro;
    - Coinvolgimento/gestione dei rapporti con i soggetti pubblici che riguardano la salute e la sicurezza sul lavoro (sul punto si rimanda alla Parte Speciale A relativa ai reati contro la Pubblica Amministrazione);
    - Gestione degli approvvigionamenti correlati all'adeguamento dei luoghi di lavoro rispetto a quanto previsto dalla legge;
    - Gestione o coinvolgimenti in attività da svolgersi in regime di appalto con riferimento agli adempimenti previsti dall'art. 26 TUS e, in particolare, individuazione delle lavorazioni e redazione dl Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI);
    - Rapporti con i fornitori coinvolti nella gestione della salute e della sicurezza sul lavoro e gestione degli acquisti di dispositivi di protezione, collettivi ed individuali, e di tutti i beni che possano influire sulla sicurezza.

Eventuali integrazioni delle suddette Aree a Rischio Reato, nonché delle relative specificazioni correlate a singoli adempimenti, potranno essere proposte al Consiglio di Amministrazione, dall'OdV e dagli organi di controllo di Teleippica, per effetto dell'evoluzione dell'attività di impresa e conseguentemente ad eventuali modifiche dell'attività svolta dalle singole sedi operative aziendali.

Costituiscono in ogni caso aree sensibili, ai fini della salvaguardia della sicurezza e salubrità nel luogo di lavoro, tutte le decisioni di politica aziendale che definiscono gli impegni di Teleippica in questo settore con riferimento, in particolare, agli obiettivi prefissati in sede di riunione periodica di cui all'art. 35 TUS, i cui verbali devono, pertanto, considerarsi parte integrante del presente Modello.

Le scelte organizzative aziendali devono essere tali da assicurare la miglior competenza e professionalità dei soggetti incaricati a vario titolo di garantire la sicurezza e salubrità del luogo di lavoro, nonché piena certezza circa i compiti e le deleghe loro conferite.
Tali processi sono formalizzati dalla Società e sono periodicamente sottoposti a monitoraggio da parte dell'OdV.

4. Norme generali di comportamento nelle aree a rischio reato

Si riportano qui di seguito i principi di comportamento che si richiede vengano adottati da parte di tutto il personale aziendale nello svolgimento delle attività attinenti alla normativa sulla salute e la sicurezza sul lavoro.
Tali regole di condotta sono finalizzate a limitare il più possibile il verificarsi dei reati previsti nel D.Lgs. 231/01.
I principi di comportamento si applicano direttamente a chiunque sia tenuto, in via diretta od indiretta, all'osservanza delle norme antinfortunistiche. La normativa vigente individua, nell'ambito dell'organizzazione aziendale, i seguenti soggetti quali garanti *ex lege*, per quanto di rispettiva competenza, dell'obbligo di sicurezza: Datore di Lavoro, dirigenti, preposti, lavoratori.

In particolare, sono indelegabili da parte del Datore di Lavoro i seguenti obblighi previsti ex art. 17, TUS:

- ***a) la valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'art. 28, TUS;***
- ***b) la designazione del responsabile di prevenzione e protezione dai rischi.***

Fatta eccezione per quanto stabilito dall'art. 17, TUS, attraverso lo strumento della delega di funzioni previsto dall'art. 16, TUS, il Datore di Lavoro può delegare, nel rispetto delle condizioni dettate dall'art.16[1], TUS, l'esecuzione degli obblighi di sicurezza a soggetti che siano dotati delle necessarie competenze.
I soggetti Delegati dal Datore di Lavoro possono a loro volta subdelegare l'esecuzione degli obblighi di sicurezza, nei limiti previsti dall'art. 16, comma 3-bis, TUS.
Datore di Lavoro e dirigenti sono tenuti all'adempimento degli obblighi previsti dall'articolo 18[2], TUS, nel quadro della più ampia previsione dell'art. 2087 cc, qualificata quale norma di chiusura

[1] Articolo 16, TUS, Delega di funzioni

1. La delega di funzioni da parte del Datore di Lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni:
   a) che essa risulti da atto scritto recante data certa;
   b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
   c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
   d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
   e) che la delega sia accettata dal delegato per iscritto.
2. La delega di funzioni di cui al comma 1 deve essere data adeguata e tempestiva pubblicità.
   f) 3. La delega di funzioni non esclude l'obbligo di vigilanza in capo al Datore di Lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. L'obbligo di cui al precedente periodo si intende assolto in caso di adozione ed efficace attuazione del modello di verifica di cui all'articolo 30, comma 4.
   g) 3 – bis Il soggetto delegato può, a sua volta, previa intesa con il Datore di Lavoro delegare specifiche funzioni in materia di salute e sicurezza sul lavoro alle condizioni di cui ai commi 1 e 2. La delega di funzioni di cui al periodo precedente non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale sia stata conferita la delega di cui al presente comma non può, a sua volta, delegare le funzioni delegate.

2 Articolo 18, TUS Obblighi del Datore di Lavoro e del dirigente

1. Il Datore di Lavoro, che esercita le attività di cui all'articolo 3, e i dirigenti, che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono:

   a) nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal presente decreto legislativo.
   b) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;

c) nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;
d) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;
e) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
f) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;
g) inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richieder al medico competente l'osservanza degli obblighi previsti a suo carico nel presente decreto;
g-bis) nei casi di sorveglianza sanitaria di cui all'articolo 41, comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro;
h) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
i) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
l) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37;
m) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
n) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;
o) consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), anche su supporto informatico come previsto dall'articolo 53, comma 5, nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r). Il documento è consultato esclusivamente in azienda.
p) elaborare il documento di cui all'articolo 26, comma 3, anche su supporto informatico come previsto dall'articolo 53, comma 5, e, , su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza. Il documento è consultato esclusivamente in azienda.;
q) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;
r) comunicare in via telematica all'INAIL, o all'IPSEMA, nonché per il loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del certificato medico, ai fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza al lavoro superiore a tre giorni. L'obbligo di comunicazione degli infortuni che comportino un'assenza dal lavoro superiore a tre giorni si considera comunque assolto per mezzo della denuncia di cui all'articolo 53 del decreto del Presidente della Repubblica 30 giugno 1965, n. 1124;
s) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50;
t) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;
u) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del Datore di Lavoro;
v) nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'articolo 35;
z) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

aa) comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza; in fase di prima applicazione l'obbligo di cui alla presente lettera riguarda i nominativi dei rappresentanti dei lavoratori per la sicurezza già eletti o designati;
bb) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità;

1-bis L'obbligo di cui alla lettera r) del comma 1, relativo alla comunicazione a fini statistici e informativi dei dati relativi agli infortuni che comportano l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento, escluso quello dell'evento, decorre dalla scadenza del termine di sei mesi dall'adozione del decreto interministeriale di cui all'articolo 8, comma 4.

2. Il Datore di Lavoro fornisce al servizio di prevenzione e protezione ed al medico competente informazioni in merito a:
a) la natura dei rischi;
b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
c) la descrizione degli impianti e dei processi produttivi;
d) i dati di cui al comma 1, lettera r), e quelli relativi alle malattie professionali;
e) i provvedimenti adottati dagli organi di vigilanza.

3. Gli obblighi relativi agli interventi strutturali e di manutenzione necessari per assicurare, ai sensi del presente decreto legislativo, la sicurezza dei locali e degli edifici assegnati in uso a pubbliche amministrazioni o a pubblici uffici, ivi comprese le istituzioni scolastiche ed educative, restano a carico dell'amministrazione tenuta, per effetto di norme o convenzioni, alla loro fornitura e manutenzione. In tale caso gli obblighi previsti dal presente decreto legislativo, relativamente ai predetti interventi, si intendono assolti, da parte dei dirigenti o

del sistema con riferimento alla portata degli obblighi di sicurezza posti *ex lege* in capo al Datore di Lavoro.

In particolare Datore di Lavoro e dirigenti sono tenuti a vigilare in ordine all'adempimento degli obblighi di sicurezza posti dalla normativa in capo a preposti, lavoratori, progettisti, fabbricanti, fornitori e, installatori e medici competenti.

Gli obblighi di sicurezza posti dalla normativa vigente in capo a preposti e lavoratori sono compiutamente disciplinati rispettivamente dagli articoli 19[3] e 20[4] TUS. In base al disposto

---

funzionari preposti agli uffici interessati, con la richiesta del loro adempimento all'amministrazione competente o al soggetto che ne ha l'obbligo giuridico.

3-bis. Il Datore di Lavoro e i dirigenti sono tenuti altresì a vigilare in ordine all'adempimento degli obblighi di cui agli articoli 19, 20, 22, 23, 24 e 25 del presente decreto, ferma restando l'esclusiva responsabilità dei soggetti obbligati ai sensi dei medesimi articoli qualora la mancata attuazione dei predetti obblighi sia addebitabile unicamente agli stessi e non sia riscontrabile un difetto di vigilanza del Datore di Lavoro e dei dirigenti.

3 Articolo 19, TUS Obblighi del preposto

1. In riferimento alle attività indicate all'articolo 3, i preposti, secondo le loro attribuzioni e competenze, devono:

a) sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di persistenza della inosservanza, informare i loro superiori diretti;

b) verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;

c) richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

d) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

e) astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;

f) segnalare tempestivamente al Datore di Lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;

g) frequentare appositi corsi di formazione secondo quanto previsto dall'articolo 37.

4 Articolo 20, TUS Obblighi dei lavoratori

1. Ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal Datore di Lavoro.

2. I lavoratori devono in particolare:

a) contribuire, insieme al Datore di Lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

b) osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;

c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;

d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;

e) segnalare immediatamente al Datore di Lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché' qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;

dell'articolo 31, TUS, il Datore di Lavoro organizza il servizio di prevenzione e protezione all'interno dell'azienda o dell'unità produttiva, o incarica persone o servizi esterni, in assenza di dipendenti che all'interno dell'azienda ovvero dell'unità produttiva, siano in possesso delle capacità e dei requisiti professionali di cui all'articolo 32, TUS.

---

f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;

g) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;

h) partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;

i) sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.

3. I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del Datore di Lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi.

5. Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto, per tutti i Destinatari del Modello adottato da Teleippica di:

- porre in essere comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, fattispecie di reato rientranti tra quelle sopra considerate (art. 25-*septies* del D.Lgs. 231/01);
- porre in essere comportamenti imprudenti, negligenti od imperiti che possano costituire un pericolo per la sicurezza all'interno dei luoghi di lavoro;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- rifiutare di utilizzare dispositivi di protezione individuale o collettivi o svolgere attività lavorative in violazione delle disposizioni impartite dai responsabili per la sicurezza;
- svolgere attività di lavoro e adoperare macchinari e strumentazioni senza aver preventivamente ricevuto adeguate istruzioni sulle modalità operative oppure senza aver precedentemente partecipato a corsi di formazione;
- omettere la segnalazione della propria eventuale incapacità o inesperienza nell'uso di strumenti aziendali;
- rifiutarsi di partecipare a corsi di formazione in materia di salute e sicurezza sul luogo di lavoro.

Sotto l'aspetto generale, nell'ambito dei suddetti comportamenti i soggetti aziendali preposti all'attuazione delle misure di sicurezza - ciascuno per le attività di sua competenza specificamente individuate - sono tenuti ad assicurare:

a) l'attuazione delle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
b) il corretto svolgimento delle riunioni periodiche di sicurezza e delle consultazioni dei rappresentanti dei lavoratori per la sicurezza;
c) le attività di sorveglianza sanitaria;
d) le attività di formazione e informazione del personale;
e) le attività di vigilanza con riferimento al rispetto delle Procedure e delle istruzioni di lavoro in sicurezza da parte del personale;
f) l'acquisizione della documentazioni e delle certificazioni obbligatorie di legge;
g) le verifiche periodiche dell'applicazione e dell'efficacia delle Procedure adottate.

Al fine di realizzare un sistema di gestione della sicurezza sul lavoro coerente, che integri al suo interno la tecnica, l'organizzazione e le condizioni del lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro, Teleippica provvede a predisporre:

- un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema sanzionatorio

idoneo a sanzionare il mancato rispetto delle misure indicate nel modello, secondo i dettami stabiliti dalle normative vigenti;

- un idoneo sistema di controllo sull'attuazione degli obiettivi prefissati in materia di sicurezza e del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- idonei sistemi di registrazione dell'avvenuta effettuazione: (i) delle attività di cui ai precedenti punti da a) ad g), (ii) delle attività oggetto delle Procedure adottate dalla Società, (iii) dei controlli effettuati, (iv) delle decisioni assunte dalla Società in materia di salute, sicurezza e igiene sul lavoro, (v) delle modalità di gestione delle risorse finanziarie in materia di salute, sicurezza e igiene sul lavoro.

Il presente allegato prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni o omissioni, conformemente alla loro formazione ed alle istruzioni e ai mezzi forniti dal Datore di Lavoro;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai soggetti preposti alla sicurezza ai fini della protezione collettiva ed individuale;
- utilizzare correttamente le apparecchiature e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a disposizione;
- segnalare immediatamente al Datore di Lavoro, al Servizio di Prevenzione e Protezione ed agli altri soggetti coinvolti nel sistema di gestione della sicurezza, le deficienze dei mezzi e dispositivi di cui ai punti che precedono, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- non rimuovere o modificare senza autorizzazione o comunque compromettere i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di propria competenza, ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- sottoporsi ai controlli sanitari previsti;
- contribuire, insieme al Datore di Lavoro, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

In particolare, con riferimento ai Terzi:

- gli ***appaltatori*** devono: (i) garantire la propria idoneità tecnico-professionale con riferimento ai lavori da eseguire; (ii) recepire le informazioni fornite da Teleippica in merito ai rischi presenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate dalla Società; (iii) cooperare e coordinarsi con

Teleippica per l'individuazione e l'attuazione delle misure di prevenzione e protezione e degli interventi necessari al fine di prevenire i rischi sul lavoro a cui sono esposti i soggetti coinvolti, anche indirettamente, nell'esecuzione dei lavori da eseguire in appalto o mediante contratto d'opera o di somministrazione;

- i ***fornitori*** devono vendere, noleggiare e concedere in uso esclusivamente strumenti ed attrezzature di lavoro, dispositivi di protezione individuali ed impianti che siano conformi alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro;

- gli ***installatori***, infine, devono attenersi alle istruzioni fornite dai fabbricanti dei prodotti da installare, con particolare riferimento alle misure e agli adempimenti in materia di salute e sicurezza sul lavoro.

In generale tutti i Destinatari del Modello devono rispettare quanto definito al fine di preservare la sicurezza e la salute dei lavoratori e comunicare tempestivamente alle strutture interne competenti eventuali segnali di rischio e/o pericolo, incidenti (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e delle Procedure aziendali.

6. Controlli specifici implementati dalla Società per il presidio delle aree a rischio

Valutazione delle politiche relative alla Salute e Sicurezza - Definizione degli obiettivi e dei programmi in materia di Salute e Sicurezza

La Società ha provveduto alla definizione della politica aziendale in tema di tutela della Salute e Sicurezza sul lavoro, nel rispetto delle leggi e dei regolamenti vigenti.

In particolare, Teleippica effettua un monitoraggio costante sui temi afferenti Salute e Sicurezza, al di là degli obblighi di legge e della prevenzione dei rischi imminenti.

Definizione del Codice Etico con indicazioni circa la politica aziendale in materia di Salute e Sicurezza

La Società ha adottato, con apposita delibera, un Codice Etico aziendale che, oltre ad avere come principio imprescindibile il rispetto di leggi e regolamenti vigenti, contiene delle specifiche indicazioni sulle tematiche relative alla salute e sicurezza sul lavoro.

Il Codice Etico adottato da Teleippica prevede specifici riferimenti ai reati di cui all'art. 25-*septies* (omicidio colposo e lesioni gravi o gravissime commesse in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro).

L'osservanza ed il funzionamento del Codice Etico è demandata all'Organismo di Vigilanza di Teleippica.
In particolare, è responsabilità dell'Organismo di Vigilanza la segnalazione di eventuali illeciti in merito a violazioni delle norme in materia di salute e sicurezza.

L'Organismo di Vigilanza rileva le eventuali violazioni segnalandole all'Organo Direttivo, cui spetta la contestazione ai trasgressori, irrogando loro le sanzioni previste dal sistema sanzionatorio adottato dalla Società, in funzione della tipologia di trasgressione e previo il necessario coordinamento con gli Organi Sociali e con le Organizzazioni Sindacali.

La Società ha definito dei programmi e degli obiettivi quantificabili coerenti con la politica della salute e sicurezza sul lavoro.

Applicazione di metodologie di identificazione e valutazione dei rischi

La modalità di identificazione dei rischi sono formalmente definite all'interno del documento DVR "Documento concernente la valutazione dei rischi per la salute e sicurezza delle persone nei luoghi di lavoro - D.Lgs. del 09/04/2008, N° 81 e smi, articolo 17" di Teleippica.

La valutazione del rischio è suddivisa nelle seguenti fasi:
1. *Identificazione delle sorgenti di rischio;*
2. *Identificazione dei rischi di esposizione;*

3. Stima dei rischi di esposizione.

I rischi sono, inoltre, suddivisi, all'interno del DVR, a seconda del livello di gravità e delle mansioni aziendali ricoperte.

All'interno del DVR sono individuate le mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.
Inoltre, il DVR riporta la descrizione del ciclo produttivo, l'individuazione delle mansioni e l'elenco delle tipologie di rischio, in considerazione anche della peculiarità delle attività svolte.
La Società ha provveduto alla valutazione dell'esistenza dei rischi, della loro entità ed ha provveduto alla definizione di un Programma di prevenzione integrata.

Individuazione dei dispositivi di prevenzione individuale

La Società, sulla base delle indicazioni del RSPP e del Medico Competente, fornisce ai lavoratori i necessari ed idonei Dispositivi di Protezione Individuale.

La Società richiede ai lavoratori l'osservanza delle normative vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei Dispositivi di Protezione Individuali (DPI) messi a loro disposizione.

Miglioramento nel tempo dei livelli di sicurezza

Al fine di garantire un miglioramento continuo in materia di salute e sicurezza sul lavoro, sono previste delle riunioni periodiche del Comitato per la sicurezza (Art. 35) in cui vengono discussi tutti gli interventi attinenti a salute e sicurezza, cui partecipano il DdL, il RSPP, il MC e i RLS.

In tali riunioni vengono definiti e formalizzati gli obiettivi da perseguire in tema di miglioramento continuo e le modalità di attuazione degli interventi per il raggiungimento degli stessi.

Nel rispetto del programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, secondo quanto disposto dall'art. 28 comma 2, lettera a), dovranno essere elencate tutte le tipologie di corsi di formazione che l'azienda ha in programma di realizzare, con l'indicazione dei tempi di attuazione.

Al fine di garantire il miglioramento dei livelli di sicurezza degli ambienti di lavoro, il DVR prevede, oltre alle misure di prevenzione e protezione, appropriate misure per il miglioramento nel tempo dei sistemi di sicurezza.

Gestione della attività di manutenzione ordinaria e straordinaria
In caso di contratti in appalto, Teleippica consegna agli appaltatori un DUVRI, finalizzato alla valutazione e conseguente gestione dei rischi interferenziali.

Monitoraggio degli infortuni e degli incidenti

La Società mantiene un registro infortuni debitamente vidimato dall'Ente di Controllo.

Definizione della struttura organizzativa, dei ruoli e delle responsabilità in materia di salute e sicurezza

Teleippica ha formalizzato e diffuso un organigramma aziendale in cui vi è evidenza della struttura di Prevenzione e Protezione in materia di Salute e Sicurezza.

La Società:

- ha identificato, nel rispetto di quanto previsto dall'articolo 2, comma 1, lett. b)[5] TUS, il Datore di Lavoro;
- ha provveduto alla valutazione dei rischi ed alla nomina dei Responsabili del Servizio di Prevenzione e Protezione ("RSPP"), dotati delle necessarie conoscenze e competenze tecniche.

Il Datore di Lavoro ha altresì provveduto ad incaricare il Responsabile al Servizio Prevenzione e Protezione, i cui compiti sono definiti nella lettera di designazione formale di nomina del RSPP.
La lettera di nomina del RSPP è firmata dal Datore di lavoro e, per accettazione dal RSPP.

Nel rispetto dei requisiti prescritti dall'art. 47 TUS, sono stati eletti i Rappresentanti dei Lavoratori per la Sicurezza (RLS), cui è stata regolarmente impartita la formazione prevista dall'art. 37 TUS.
La Società ha diffuso, attraverso le comunicazioni interne "Designazione degli addetti incaricati alla gestione delle emergenze", la nomina dei lavoratori incaricati alla gestione delle emergenze.

Gestione del personale in materia di Salute e Sicurezza - Diffusione del sistema sanzionatorio ai dipendenti

Il sistema sanzionatorio di Teleippica è redatto in conformità con il CCNL, ed è reso noto a tutti i dipendenti al momento dell'assunzione.

Il sistema sanzionatorio nell'ambito del Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/01 è comunicato, attraverso programmi di formazione e informazione a tutto il personale dipendente e dirigenziale di Teleippica.

Nello specifico:

- per i <u>dirigenti e soggetti con funzione di rappresentanza,</u> è prevista una formazione iniziale attraverso riunioni *ad hoc* nel periodo immediatamente successivo all'approvazione del Modello e la diffusione di documentazione in argomento, con comunicazione costante e tempestiva di eventuali aggiornamenti e modifiche.

[5] Ai fini ed agli effetti delle disposizioni di cui al presente decreto legislativo si intende per «Datore di Lavoro»: "*il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa. Nelle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, per Datore di Lavoro si intende il dirigente al quale spettano i poteri di gestione, ovvero il funzionario non avente qualifica dirigenziale, nei soli casi in cui quest'ultimo sia preposto ad un ufficio avente autonomia gestionale, individuato dall'organo di vertice delle singole amministrazioni tenendo conto dell'ubicazione e dell'ambito funzionale degli uffici nei quali viene svolta l'attività, e dotato di autonomi poteri decisionali e di spesa. In caso di omessa individuazione, o di individuazione non conforme ai criteri sopra indicati, il Datore di Lavoro coincide con l'organo di vertice medesimo*".

- per il personale dipendente, è prevista la comunicazione di informativa interna esplicativa del Modello e del relativo sistema sanzionatorio, una specifica informativa viene impartita ai neoassunti.

Teleippica promuove la conoscenza e l'osservanza del Modello e del relativo sistema sanzionatorio, anche tra i partner commerciali e collaboratori esterni.

La Società provvede ad informare i soggetti esterni sul contenuto del Modello. Inoltre, i contratti e qualsiasi tipo di accordo commerciale contengono specifiche clausole con cui i collaboratori ed i partners si impegnano al rispetto delle norme contenute nel Modello, con la previsione di una clausola risolutiva espressa tramite la quale il contratto o l'accordo commerciale si risolverà di diritto nel caso in cui non venissero rispettate le disposizioni del Modello stesso.

Attività di formazione verso il personale

La Società ha predisposto un Piano di formazione per i lavoratori, e per i principali soggetti coinvolti in materia di salute e sicurezza sul lavoro.

All'interno del Piano di Formazione sono previste le tematiche e le tempistiche degli interventi formativi per tutto il personale dipendente.

Al dipendente al momento dell'assunzione viene consegnata la documentazione afferente le tematiche sulla sicurezza, controfirmata dallo stesso per accettazione.

Sorveglianza Sanitaria - Predisposizione del piano di Sorveglianza Sanitaria

Al fine di assolvere agli adempimenti previsti dagli artt. 38 ss. TUS in materia di sorveglianza sanitaria, Teleippica ha designato il Medico Competente con espressa accettazione dell'incarico da parte dello stesso.

Annualmente viene predisposto un Piano di Sorveglianza Sanitaria, proposto dal Medico Competente.
All'interno del Piano sono indicate tutte le visite mediche sostenute dai dipendenti della Società nell'anno di riferimento.
Il Piano di sorveglianza Sanitaria prevede visite mediche periodiche, da parte del Medico Competente e, se giudicato necessario da quest'ultimo, da Specialisti, nonché controlli periodici mediante monitoraggi biologici e strumentali.
E' responsabilità del Datore di Lavoro inviare i lavoratori alla visita medica entro le scadenze previste all'interno del Piano.

Il Medico Competente provvede, inoltre, alla redazione di un report annuale sulle attività di sorveglianza sanitaria per l'anno di riferimento.
I risultati consuntivi dell'attività sono forniti al Datore di Lavoro, al RSPP e ai RLS in occasione della riunione periodica di sicurezza ex-art.35 ai sensi dell'art. 25, comma 1 lett. I) del D.Lgs. 81/08.
Tali attività sono finalizzate alla programmazione e all'attuazione di misure di tutela della salute e della integrità psico-fisica dei lavoratori.

Il medico competente istituisce per ogni lavoratore sottoposto a sorveglianza sanitaria, una cartella sanitaria e di rischio. Tale cartella è conservata con salvaguardia del segreto professionale e, salvo il tempo strettamente necessario per l'esecuzione della sorveglianza sanitaria e la trascrizione dei relativi risultati, presso il luogo di custodia concordato al momento della nomina del medico competente.

Tracciabilità delle informazioni - Archiviazione della documentazione afferente la Salute e la Sicurezza

I documenti archiviati sono identificabili adeguatamente ed è individuato un punto di custodia "Armadio della Sicurezza" della documentazione in ambito SSL.

Riesame del Sistema - Monitoraggio continuo sul Sistema di Salute e Sicurezza

Il Datore di Lavoro indice almeno una volta l'anno la Riunione Periodica di Prevenzione e Protezione dai Rischi, ai sensi dell'art.35 del DLgs 81/2008.

Tali riunioni periodiche vengono formalizzate nell'apposito documento "Verbale di riunione periodica di prevenzione e protezione dai rischi (comma 1 art. 35 D.Lgs. 81/2008), che prevede:

a) elenco partecipanti (DdL, RSPP, MC, RLS, eventuali consulenti esterni per salute e sicurezza);
b) argomenti all'ordine del giorno (stato di avanzamento delle misure di miglioramento previste, stato di avanzamento dei programmi di informazione e formazione dei lavoratori ai fini della sicurezza, esiti delle verifiche presso gli ambienti di lavoro, analisi dell'andamento del fenomeno infortunistico, aggiornamento sui rischi).

Le riunioni hanno altresì luogo in occasione di eventuali significative variazioni delle condizioni di esposizione al rischio, compresa la programmazione e l'introduzione di nuove tecnologie che hanno riflessi sulla sicurezza e salute dei lavoratori.

7. Compiti dell'OdV

Fermi restando i compiti e le funzioni dell'Organismo di Vigilanza statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati in materia di salute e sicurezza sul lavoro lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire il verificarsi di eventi lesivi per i Lavoratori;
- predisporre e aggiornare apposite procedure interne volte a definire le modalità ed i termini per l'acquisizione e la trasmissione dei dati informativi relativi agli infortuni sul lavoro;
- predisporre, con l'ausilio degli altri soggetti coinvolti, un sistema di flussi informativi che consenta la circolazione delle informazioni all'interno dell'azienda, al fine sia di favorire il coinvolgimento e la consapevolezza di tutti i Destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, sia di assicurare la tempestiva ed adeguata evidenza di eventuali carenze o violazioni del Modello, ovvero degli interventi necessari al suo aggiornamento;
- effettuare una periodica attività di monitoraggio della funzionalità del complessivo sistema preventivo adottato dalla Società con riferimento al settore della salute e della sicurezza sul lavoro. A tali fini, deve essere inviata all'OdV copia della reportistica periodica in materia di salute e sicurezza sul lavoro prevista dalla normativa e dalle procedure aziendali, e segnatamente il verbale della riunione periodica di cui all'art. 35 del TU, nonché tutti i dati relativi agli infortuni sul lavoro occorsi nella Società;
- promuovere il costante aggiornamento del Modello 231 e del sistema preventivo adottato dalla Società, con l'ausilio dei soggetti coinvolti, al fine di assicurare il costante miglioramento del grado di sicurezza. In particolare l'efficacia e l'adeguatezza delle misure di prevenzione e protezione devono essere periodicamente monitorate. Tali misure devono essere sostituite, modificate o aggiornate qualora ne sia riscontrata l'inefficacia e/o l'inadeguatezza, anche parziali, ovvero in relazione ad eventuali mutamenti organizzativi e dei rischi. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- monitorare il regolare svolgimento e la partecipazione ai corsi in materia di salute, igiene e sicurezza sul lavoro.

L'OdV svolge in piena autonomia le proprie attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici e/o a campione sulle attività connesse ai Reati in materia di salute e sicurezza sul lavoro al fine di verificare la corretta implementazione delle stesse in relazione alle regole previste dal Modello.

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

L'OdV comunica i risultati della propria attività di controllo relativamente ai Reati in materia di salute e sicurezza sul lavoro al Consiglio di Amministrazione e al Collegio Sindacale secondo quanto previsto nella Parte Generale del Modello.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale D

Delitti Informatici e Trattamento Illecito Dei Dati
(Art. 24-bis D.Lgs. 231/2001)

TELEIPPICA SRL

INDICE

1. Premessa

La presente Parte Speciale riguarda i reati previsti dall'articolo 24-*bis* del D.Lgs. n. 231/2001 (qui di seguito anche il "Decreto") che è stato inserito nel Decreto ad opera della legge 18 marzo 2008, n. 48, recante "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest 23 novembre 2001) e norme di adeguamento dell'ordinamento interno".

La presente Parte Speciale concerne, in particolare, i comportamenti che devono essere tenuti dai soggetti - Amministratori e personale in posizione apicale operante in nome e per conto della Società, dirigenti e dipendenti di Teleippica S.r.l. (di seguito anche "*Teleippica*" o "*Società*") anche per il tramite di fornitori, consulenti che svolgono la propria prestazione all'interno della Società, indipendentemente dalla qualificazione giuridica del loro rapporto con la Società - che sono quindi coinvolti nei processi e nelle attività sensibili ed operano pertanto nelle Aree a Rischio Reato (qui di seguito i "Destinatari").

Tutti i Destinatari della presente Parte Speciale del Modello sono tenuti ad adottare comportamenti conformi a quanto di seguito formulato al fine di prevenire la commissione dei reati individuati nell'ambito della normativa di riferimento.

2. I delitti di cui all'art. 24-bis del D.Lgs. 231/2001 – Esempi delle modalità di commissione

Con la previsione di cui all'art. 24-*bis*, il Legislatore ha previsto la responsabilità dell'ente in relazione a due tipologie di reati:
a) i reati propriamente informatici;
b) i reati di falso commessi mediante l'utilizzo di documenti/dati informatici.

2.1. Reati propriamente informatici

Con riferimento a questa prima categoria di reati, si rintracciano una serie di elementi comuni, vale a dire:

***i) elemento oggettivo*:** seppure le condotte possono essere materialmente diverse, si tratta di illeciti penali in cui il computer o il sistema informatico o telematico costituisce il fulcro della condotta. Ed infatti il computer o il sistema informatico o telematico rappresentano o il mezzo/modalità di realizzazione della condotta (condotte realizzate mediante l'uso del computer), o la natura dell'oggetto materiale (condotte realizzate contro il computer - sistema informatico o telematico).
Per "sistema informatico" si intende "*una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche*" (Cass. Sez. VI Pen, 4 ottobre - 14 dicembre 1999, n.3067): più recentemente cfr. anche Cass. Sez. V Pen., 6 febbraio 2007, n. 11689[1] Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su

1 La Convenzione di Budapest del 2001, cit., art. 1, lett. a), ha definito come sistema informatico "*qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge l'elaborazione automatica di dati attraverso l'esecuzione di un programma software*".

supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici ("codice"), in combinazioni diverse: tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite "da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente". Per "sistema telematico" si intende invece qualsiasi rete di telecomunicazione, sia pubblica che privata, nazionale o internazionale, operante da o per l'Italia.

ii) elemento soggettivo: sono tutti reati puniti a titolo di dolo (coscienza e volontà di commettere il reato), anche se per alcuni di essi è necessario anche il dolo specifico (vale a dire un'intenzione ulteriore che l'agente deve avere di mira nel compiere la condotta delittuosa: es. fine di trarre profitto).

Si riporta, di seguito, il testo delle disposizioni del Codice Penale espressamente richiamate dall'art. 24-*bis* del D.Lgs. 231/2001 ed afferenti la presente categoria di reati, che sono stati ritenuti astrattamente applicabili alla Società, unitamente ad un breve commento sulle singole fattispecie.

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

"I. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
II. La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
III. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
IV. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Tale reato si realizza quando un soggetto si introduca abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza.
A tal riguardo si sottolinea come il legislatore abbia inteso punire l'accesso non autorizzato ad un sistema informatico o telematico *tout court*, e dunque anche quando ad esempio all'accesso non segua un danneggiamento di dati (si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio, limitandosi ad eseguire una copia, oppure procedendo solo alla visualizzazione di informazioni).

La suddetta fattispecie delittuosa si realizza, altresì, nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema.
Il delitto potrebbe essere astrattamente configurabile, ad esempio, nell'ipotesi in cui un dipendente della Società acceda, abusivamente, utilizzando password indebitamente carpite, al sistema informatico di una società concorrente per prendere cognizione di dati riservati durante una negoziazione commerciale.

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

"I. Chiunque, 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 fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.
II. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater."

Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.
L'art. 615 *quater* c.p., pertanto, punisce le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.
I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici o password.
La norma punisce, inoltre, il rilascio di istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

A titolo di esempio, il reato potrebbe configurarsi nel caso in cui un dipendente della Società, una volta procuratesi le credenziali, comunichi o consegni a terzi i codici, parole chiave o altri mezzi necessari all'accesso al sistema informatico di una società concorrente.

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

"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329."

Tale reato si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso

pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.
A titolo di esempio, il reato potrebbe configurarsi qualora un dipendente della Società effettui attacchi di hacking per alterare i dati relativi, ad esempio, ai dossier dei prodotti di una società concorrente.

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

"I. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
II. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
III. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
IV. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato."

Tale ipotesi di reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.
Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o telematici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

A titolo di esempio, il reato potrebbe configurarsi nel caso in cui un dipendente della Società impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati per la partecipazione ad una trattativa.

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

"I. Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

II. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater."

Questa fattispecie di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
La condotta vietata dalla norma è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui un dipendente della Società installi dispositivi tecnologici (es. sniffer) volti ad intercettare le comunicazioni telefoniche, o informatiche di un'impresa concorrente.

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

"I. Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
II. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio."

Il reato punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

A titolo di esempio, il reato potrebbe ravvisarsi nella condotta del dipendente della Società che proceda alla eliminazione o alterazione dei file di un programma informatico di un creditore della Società, al fine, ad esempio, di far sparire dati compromettenti o di celare la prova di un credito vantato da un fornitore nei confronti della Società.

- **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.)**

"I. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
II. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
III. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Tale reato si realizza quando un soggetto commetta 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 delitto si distingue dal precedente poiché, in questo caso, viene attribuito rilievo penale non solo al danneggiamento in sé, ma anche ai fatti preparatori del danneggiamento, e si configura pertanto come reato di pericolo; inoltre, le condotte dannose hanno ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati, ma destinati al soddisfacimento di un interesse di natura pubblica.

A titolo esemplificativo, tale fattispecie potrebbe, astrattamente, realizzarsi nell'ipotesi in cui un dipendente della Società distrugga documenti informatici detenuti dall'Autorità giudiziaria relativi ad una ipotetica indagine nei confronti della Società.

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

"I. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
II. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Il reato si realizza quando un soggetto, mediante le condotte di cui all'art. 635 *bis* c.p. (e cioè la distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.
Si veda l'esempio di modalità di commissione dell'illecito indicato in corrispondenza del reato di cui all'art. 635-*bis* c.p., qualora la condotta abbia come conseguenza la distruzione, il danneggiamento o l'inservibilità di un sistema informatico o telematico altrui (per es., di un concorrente).

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

"I. Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
II. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
III. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Il reato si configura quando la condotta di cui all'art. *635*-quater c.p. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art.

635-*ter* c.p., quel che rileva è in primo luogo che il danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.
A titolo esemplificativo, tale fattispecie potrebbe astrattamente realizzarsi nell'ipotesi in cui un dipendente della Società, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, danneggi sistemi informatici o telematici dell'Autorità giudiziaria (in caso di pendenza di una ipotetica indagine nei confronti della Società).

2.2. I reati di falso commessi mediante l'utilizzo di documenti/dati informatici

Con riferimento alla categoria di reati precedentemente indicata ***sub* b)** (paragrafo 2), si rilevano i seguenti elementi comuni:

i) definizione di "documento informatico": qualunque supporto informatico contenente dati e informazioni aventi efficacia probatoria (quindi il documento informatico viene equiparato all'atto pubblico o alla scrittura privata avente efficacia probatoria);

ii) bene giuridico tutelato: il bene tutelato dalle norme è la "fede pubblica", vale a dire l'interesse a che i mezzi probatori siano genuini e veridici e alla certezza dei rapporti economici e giuridici;

iii) elemento oggettivo: questa tipologia di reati si concretizza nella condotta di alterare/manomettere il documento nella sua essenza materiale, ovvero nella sua genuinità (c.d. "falsità materiale") ovvero in condotte che tendono ad incidere sul contenuto dello stesso, vale a dire sulla verità dei fatti in esso espressi (c.d. "falsità ideologica");

iv) elemento soggettivo: i reati sono puniti solo a titolo di dolo (è esclusa quindi la punibilità per colpa - negligenza, imperizia, imprudenza inosservanza di leggi).

- **Falsità di documenti informatici (art. 491 *bis* c.p.)**

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

La norma stabilisce che i delitti di falsità in atti previsti dal Codice Penale (Capo III, Titolo VII, Libro II) sono punibili anche nel caso in cui l'oggetto della condotta sia un "documento informatico", ovvero un documento pubblico o privato, avente efficacia probatoria, in quanto rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti. Le condotte di falso astrattamente rilevanti e applicabili a Teleippica sono:

- **Falsità materiale commessa dal privato (art. 482 c.p.)**

"Se alcuno dei fatti preveduti dagli articoli 476[2], 477[3] e 478[4] è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo."

A titolo di esempio, il reato sarebbe configurabile laddove un dipendente della Società alteri le ricevute bancarie telematiche di versamenti tributari (fattispecie di cui all'art. 476 c.p.), ovvero alteri dei certificati o autorizzazioni amministrative in forma digitale (fattispecie di cui all'art. 477 c.p.), ovvero, supponendo esistente un atto pubblico o privato in forma digitale, ne simuli una copia ed il rilascio della stessa in forma legale (fattispecie di cui all'art. 478 c.p.).

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

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

Ad esempio il reato potrebbe configurarsi nel caso in cui un dipendente della Società in sede di richiesta di autorizzazioni o licenze, dichiari, per via telematica, che la Società possiede determinati requisiti necessari al fine del relativo rilascio.

- **Falsità in scrittura privata (art. 485 c.p.)**

"I. Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.
II. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata."

---

[2] Art. 476 c.p. ("Falsità materiale commessa dal pubblico ufficiale in atti pubblici"): "*I. Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.*
II. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni."

[3] Art. 477 c.p. ("Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative"): *"Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni."*

[4] Art. 478 c.p. ("Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti): *"I. Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.*
II. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.
III. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni."

Tale fattispecie è astrattamente realizzabile qualora un dipendente della Società falsifichi documenti informatici privati al fine di procurare un vantaggio per la Società.

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

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

Per quanto i commentatori siano divisi sulla possibilità di applicare la fattispecie ai documenti informatici, si ipotizza astrattamente la possibilità di realizzare la fattispecie qualora un dipendente della Società falsifichi il contenuto di documenti informatici privati dotati di firma elettronica qualificata o firma digitale, inserendovi un contenuto diverso rispetto a quello autorizzato, al fine di procurare un vantaggio per la Società.

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

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

A titolo di esempio tale fattispecie è astrattamente realizzabile qualora il dipendente della Società utilizzi documenti informatici falsi - per esempio ricevute di pagamento effettuato in via telematica falsificando i documenti, per procurare un vantaggio alla Società.

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

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

A titolo esemplificativo, la fattispecie è astrattamente realizzabile nei casi in cui il dipendente della Società acceda in un sistema informatico altrui e distrugga documenti aventi efficacia probatoria.

- **Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)**

"Agli effetti delle disposizioni precedenti, nella denominazione di «atti pubblici» e di «scritture private» sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti."

Le ultime norme sopra riportate definiscono il possibile ambito di estensione oggettiva o soggettiva dei reati di falso.

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

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

Commette il reato in esame il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri in ingiusto profitto ovvero di arrecare ad altri un danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Sulla base dei risultati del *risk assessment*, il Gruppo di Lavoro ha identificato alcune fattispecie di reato previste dall'art. 24 *bis* del Decreto non applicabili alla Società, che conseguentemente non sono state sopra riportate, ovvero:

- talune fattispecie previste dal Capo III, Libro II c.p., se riguardanti un documento informatico pubblico o privato, intendendosi per tale qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli aventi efficacia probatoria (art. 491 bis c.p.), ovvero:
- falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.);
- falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.);
- falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.);
- falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.);
- falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 c.p.);
- falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.);
- falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.);
- falsità commesse da pubblici impiegati incaricati di un servizio pubblico (art. 493 c.p.).

Tale valutazione è stata assunta tenendo conto dell'attuale struttura di Teleippica dell'oggetto sociale e delle attività attualmente svolte dalla Società stessa.

3. Le sanzioni previste in relazione all'art. 24-bis del Decreto

Si riporta di seguito una tabella riepilogativa delle sanzioni a carico dell'Ente previste all'art. 24-*bis* del Decreto qualora, per effetto della commissione dei reati indicati al precedente capitolo 2 da parte dei soggetti apicali e/o dei soggetti sottoposti, derivi all'Ente un interesse o un vantaggio.

Reato	**Sanzione Pecuniaria**	**Sanzioni Interdittive**
Accesso abusivo ad un sistema informatico o telematico (615 *ter* c.p.) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 *quater* c.p.) Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617 *quinquies* c.p.) Danneggiamento di informazioni, dati e programmi informatici (635 *bis* c.p.) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635 *ter* c.p.) Danneggiamento di sistemi informatici o telematici (635 *quater* c.p.) Danneggiamento di sistemi informatici o telematici di pubblica utilità (635 *quinquies* c.p.)	Da 100 a 500 quote	Si applicano le seguenti sanzioni interdittive previste dall'art. 9, co. 2 del Decreto: a) interdizione dall'esercizio della attività; b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) divieto di pubblicizzare beni o servizi.

Reato	Sanzione Pecuniaria	Sanzioni Interdittive
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615 *quater* c.p.) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615 *quinquies* c.p.)	Fino a 300 quote	Si applicano le seguenti sanzioni interdittive previste dall'art. 9, co. 2 del Decreto: b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) divieto di pubblicizzare beni o servizi.
Documenti informatici -Falsità (491 *bis* c.p.) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 *quinquies* c.p.)	Salvo quanto previsto dall'articolo 24 del Decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, fino a 400 quote	Si applicano le seguenti sanzioni interdittive previste dall'art. 9, co. 2 del Decreto: c) divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; e) divieto di pubblicizzare beni o servizi.

Oltre alle sanzioni sopra citate va in ogni caso considerata la confisca del prezzo o del profitto del reato, sempre disposta con la sentenza di condanna, salvo che per la parte che può essere restituita al danneggiato. Quando non è possibile eseguire la confisca del prezzo o del profitto del reato, la confisca potrà avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

In caso di commissione dei reati che precedono si applica inoltre la sanzione della pubblicazione della sentenza di condanna, che può essere disposta, ai sensi dell'art. 18 del Decreto, quando nei confronti dell'ente viene applicata una sanzione interdittiva. La pubblicazione della sentenza avviene secondo le modalità di cui all'art. 36 c.p., nonché mediante affissione nel comune ove l'ente ha la sede principale.

4. Le Aree a potenziale Rischio Reato

Tra le attività sensibili ai fini dell'art. 24-bis del Decreto sono incluse tutte le attività in cui è previsto l'utilizzo di sistemi informatici e telematici e, pertanto, non è possibile aprioristicamente limitare alcun ambito di attività aziendale potenzialmente esposta al presente Rischio Reato.

Tutti i delitti sopra indicati sono reati comuni che possono essere commessi dai dipendenti della Società, i quali fanno sistematico uso di sistemi informatici e telematici; la possibilità di commetterli è pertanto trasversale alla Società stessa.
Ogni Direzione e Funzione aziendale è quindi, ai limitati fini dei reati in commento, una potenziale Area Sensibile.
Tuttavia si evidenzia, come già sopra menzionato, che la funzione IT, occupandosi precipuamente di gestione dei sistemi aziendali e attività di service management a supporto degli utenti, risulta maggiormente esposta alla commissione di tali reati.
Si rileva, tuttavia, come le aree aziendali che presuppongono l'invio di documenti informatici verso la Pubblica Amministrazione e l'Area di gestione dei sistemi informativi costituiscano le aree maggiormente esposte al rischio potenziale di incorrere nei reati di cui all'art. 24 bis del Decreto.

Eventuali integrazioni delle Aree a potenziale Rischio Reato potranno essere proposte al Consiglio di Amministrazione dall'OdV e dagli altri organi di controllo della Società per effetto dell'evoluzione dell'attività di impresa e conseguentemente ad eventuali modifiche dell'attività svolta dalle singole Direzioni/Funzioni.

4.1. Le aree a potenziale rischio reato: attività "sensibili", ruoli aziendali coinvolti, controlli a presidio

Per quanto attiene le aree aziendali nelle quali è previsto l'invio di documenti informatici alla Pubblica Amministrazione si rinvia con riferimento ai ruoli aziendali coinvolti nelle attività ed ai controlli posti in essere da Teleippica, alla Parte Speciale "Reati contro la Pubblica Amministrazione" del presente Modello. In tali aree, ai fini della presente parte speciale del Modello si individuano come Reati astrattamente ipotizzabili i reati di cui alla categoria precedentemente indicata ***sub* b)** (paragrafo 2).

Nell'ambito dell'area Gestione dei Sistemi Informativi sono, invece, di seguito individuati:

- le c.d. attività "sensibili", ossia quelle attività al cui svolgimento è potenzialmente connesso il rischio di commissione dei reati;
- i ruoli aziendali coinvolti nell'esecuzione di tali attività sensibili;
- i principali controlli previsti con riferimento alle attività poste in essere.

a) Gestione sistemi informativi

Attività sensibili:

- Gestione della sicurezza fisica e logica delle informazioni aziendali elettroniche o in forma digitale;
- Gestione della configurazione delle componenti software ed hardware installate sulle postazioni di lavoro;
- Gestione degli accessi alle apparecchiature informatiche, alla rete aziendale, alle applicazioni ed ai sistemi ed alle reti telematiche;
- Protezione dei dispositivi rimovibili (es. hard disk esterno; pen drive);
- Acquisizione, sviluppo e manutenzione dei sistemi informatici;
- Gestione dei cambiamenti degli applicativi aziendali;
- Gestione del flusso informativo verso Enti Pubblici, mediante strumenti informatici;
- Gestione delle informazioni e dei dati custoditi presso gli archivi informatici;
- Gestione degli incidenti e dei problemi di sicurezza informatica su dati ed informazioni.

Processi e ruoli aziendali coinvolti:
Gestione delle componenti software/hardware, delle reti aziendali, dei flussi informativi informatici e della custodia dei dati – Funzione ICT.

Reati astrattamente ipotizzabili ed esemplificazioni delle modalità di commissione dei reati:
Si rimanda a quanto descritto nel capitolo 2 della presente Parte Speciale.

Presidi di controlli esistenti:
Per ciò che concerne la presente Area a Rischio Reato e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che vengano commessi possibili violazioni. In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio Reato devono rispettare i principi contenuti nel Modello (Parte Generale e Parte

Speciale), nelle sue procedure, nel sistema di procure e deleghe, nel Codice Etico e di Comportamento; in via esemplificativa e non esaustiva possono essere menzionati una serie di controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei componenti software/hardware, delle reti aziendali, dei flussi informativi informatici e della custodia dei dati;
- sono state definite le responsabilità relative all'utilizzo di Internet, dei servizi di Posta Elettronica, della rete aziendale e dei telefoni in dotazione quali strumento a fini esclusivi di lavoro;
- sono presenti dei controlli automatici volti a bloccare una sessione inattiva o ad effettuare il log-off di terminali inattivi connessi alla rete aziendale;
- la Società ha definito delle procedure volte a limitare l'effetto di software dannosi e ripristinare il corretto funzionamento dei sistemi: sull'intera rete (personal computer e server) è installato un *software antivirus* ed è previsto un controllo di accesso ad internet tramite Websense;
- l'utilizzo dei servizi informatici aziendali richiede un codice di identificazione personale (*user-id*) ed una parola chiave segreta (*password*), che non può essere ceduta a terzi neppure temporaneamente;
- la Società ha definito i requisiti della password, in termini di lunghezza minima, scadenza, history, lockout e complessità della password;
- la Società ha definito i processi di ingresso di un nuovo dipendente, di dimissioni o di cambio ufficio, relativamente ai profili di accesso ai sistemi informativi;
- periodicamente è effettuata una *review* delle utenze di accesso alle applicazioni aziendali;
- l'utilizzo di internet, quale strumento ai fini esclusivi di lavoro, è autorizzato solo attraverso la rete di trasmissione dati aziendale;
- la casella di posta, è assegnata al dipendente (che è responsabile del suo corretto utilizzo) quale strumento ai fini esclusivi di lavoro. L'account di e-mail viene assegnato al dipendente su richiesta del proprio Responsabile e può essere configurato solo su un PC client di posta;
- sono posti in essere controlli volti a garantire l'integrità e l'autenticità dei dati trasmessi su reti pubbliche, quali ad esempio la firma digitale;
- sono posti in essere controlli volti a vietare l'accesso abusivo al proprio sistema telematico al fine di alterare e /o cancellare dati e/o informazioni;
- sono posti in essere controlli volti a vietare l'utilizzo abusivo di codici, parole chiave o altri mezzi idonei all'accesso a un sistema telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- è disposto l'assoluto divieto di procedere all'installazione di qualsiasi *software* o *hardware* senza preventiva autorizzazione;
- la Società è dotata di firewall;
- le connessioni da remoto verso la intranet aziendale sono gestite attraverso il protocollo standard VPN (Virtual Private Network);
- le macchine server sono custodite all'interno di sale server il cui accesso è limitato;
- la Società ha disposto che l'utilizzo di dispositivi rimovibili (floppy disk, cd rom, cd riscrivibili, nastri magnetici, chiavi USB) può avvenire solo previa autorizzazione.

5. Principi e regole di comportamento

Tutte le attività ricomprese nell'Area a Rischio Reato devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure di Teleippica, nonché le regole contenute nel presente Modello.
Inoltre, i Destinatari del Modello devono ispirare la loro azione ai seguenti principi:

- *riservatezza:* garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- *integrità:* garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico o telematico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano tracciate e trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- *disponibilità:* garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

5.1. Principi e regole particolari di comportamento

E' fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato previste dall'articolo 24-bis del D.Lgs. 231/2001.
Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico dei Destinatari di Teleippica (limitatamente e rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- utilizzare utenze con accesso amministrativo per attività estranee all'amministrazione dei sistemi informativi.

Pertanto, tutti coloro i quali operano per Teleippica devono:

- non prestare o cedere a Terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile;
- segnalare al Responsabile della propria Funzione, il furto, il danneggiamento o lo smarrimento di tali strumenti, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo;
- evitare di introdurre e/o conservare in Azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;
- evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici e telematici.

6. Compiti dell'OdV

Fermi restando i compiti e le funzioni dell'Organismo di Vigilanza statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Delitti Informatici e trattamento illecito dei dati, lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei Delitti Informatici e trattamento illecito dei dati, previsti dal Decreto;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV svolge in piena autonomia le proprie attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici e/o a campione sulle attività connesse ai Delitti Informatici e trattamento illecito dei dati al fine di verificare la corretta implementazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'OdV, viene garantito libero accesso a tutta la documentazione aziendale rilevante.

L'OdV comunica i risultati della propria attività di controllo relativamente ai Delitti Informatici e trattamento illecito dei dati al Consiglio di Amministrazione e al Collegio Sindacale secondo le modalità definite dalla Parte Generale del Modello.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale E

Reati in materia di violazione del diritto d'autore
(Art. 25-novies D.Lgs. 231/2001)

TELEIPPICA SRL

INDICE

1. I delitti di cui all'art. 25-novies del D.Lgs. 231/2001

I reati in materia di violazione del diritto d'autore sono stati introdotti dalla Legge speciale n. 633/1941 (e sue successive integrazioni/modificazioni) e recepiti all'interno del D.Lgs. 231/01 con la Legge 99/2009.

La citata Legge 633/1941, prevede i seguenti reati:

- messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171 L.633/1941 comma 1 lett. a) bis);
- reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, L.633/1941 comma 3);
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis L.633/1941 comma 1);
- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis L.633/1941 comma 2);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter L.633/1941);
- mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies L.633/1941);
- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies L.633/1941).

In particolare, in considerazione dell'attività svolta da Teleippica S.r.l. (di seguito "*Teleippica*" o "*Società*"), la Società ha ritenuto rilevanti le seguenti fattispecie di reato, di cui viene riportato il testo integrale, unitamente ad un breve commento e all'esemplificazione delle possibili modalità di commissione:

- **Art. 171 bis 1 e 2 comma L. 633/1941**

"Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da € 2.582 a € 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a € 15.493 se il fatto è di rilevante gravità".

"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 in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il re-impiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da € 2.582 a € 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità".

Il primo comma dell'art. 171-*bis* è volto a tutelare penalmente il c.d. *software*, punendo l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore; ma anche l'importazione, la distribuzione, la vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; è altresì punita la predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.
La condotta può consistere anzitutto nella abusiva duplicazione, essendo prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro.
La seconda parte del comma indica le altre condotte che possono integrare il reato *de quo*: importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi "piratati". Si tratta di condotte caratterizzate dall'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale.
Infine, nell'ultima parte del comma, il legislatore ha inteso inserire una norma volta ad anticipare la tutela penale del software, punendo condotte aventi ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui l'Ente acquisti una singola licenza per un programma e provveda alla sua duplicazione, in modo da distribuire tali programmi al proprio interno e/o commercializzare tali programmi all'esterno.

Il comma 2 dell'art. 171-*bis* mira alla protezione delle banche dati; la condotta, invero, si concretizza nella riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; nell'estrazione o reimpiego della banca dati; nella distribuzione, vendita o concessione in locazione di banche di dati.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui la Società, attraverso l'accesso a banche dati online riproduca in tutto o in parte opere, testi ecc, al fine di trarne un vantaggio in termini di immagine e pubblicità.

- **Art. 171 ter L. 633/1941**

1) "È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da € 2.582 a € 15.493 chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata 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, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, 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;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

g) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei

titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche 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.

2) È punito con la reclusione da uno a quattro anni e con la multa da da euro 2.582 a euro 15.493 chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

b) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

c) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

d) promuove o organizza le attività illecite di cui al comma 1.

3) La pena è diminuita se il fatto è di particolare tenuità.

4) La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5) Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici".

La norma punisce l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; la riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui la Società riproduca abusivamente opere o parti di opere musicali, al fine di trarne un profitto.

- **Art. 171 septies L. 633/1941**

"La pena di cui all'articolo 171-ter, comma 1, si applica anche:

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge".

Il reato si configura allorquando i produttori ed importatori dei supporti non soggetti a contrassegno SIAE non comunichino alla SIAE stessa, entro 30 giorni dalla commercializzazione o dall'importazione, i dati necessari per l'univoca identificazione dei supporti medesimi, nonché qualora si dichiari falsamente l'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi.

2. Le sanzioni previste in relazione alle disposizioni di cui all'articolo 25-novies del D.Lgs. 231/01

Si riporta, di seguito, una tabella riepilogativa delle sanzioni previste dall'art. 25-novies, del D. Lgs. n. 231/01, elencati al precedente paragrafo 1.

Reato di cui all'art.25 novies	**Sanzione Pecuniaria**	**Sanzione Interdittiva**
• Art. 171, co. 1, lett. a-bis), Legge 22 aprile 1941, n. 633; • Art. 171, co. 3, Legge 22 aprile 1941, n. 633; • Art. 171-*bis*, Legge 22 aprile 1941, n. 633; • Art. 171-*ter*, Legge 22 aprile 1941, n. 633; • Art. 171-*septies*, Legge 22 aprile 1941, n. 633; • Art. 171-*octies*, Legge 22 aprile 1941, n. 633	Fino a 500 quote	Per una durata non superiore ad un anno: • interdizione all'esercizio dell'attività; • sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; • il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; • esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; • divieto di pubblicizzare beni o servizi. Fatto salvo quanto previsto dall'art. 174-*quinquies,* Legge 22 aprile 1941, n. 633.

3. Le Aree a potenziale Rischio Reato

Con riferimento alle fattispecie di reato richiamate dall'art. 25-*novies* del D. Lgs. n. 231/2001 e ritenute rilevanti per Teleippica, sono state individuate le Aree a Rischio, le relative attività sensibili, i ruoli aziendali coinvolti e le possibili modalità di commissione del reato.
Si riporta, di seguito, l'indicazione delle Aree a Rischio individuate in relazione ai reati in materia di violazione del diritto d'autore:

- Gestione dei sistemi informativi;
- Gestione dei contenuti editoriali.

Eventuali integrazioni delle suddette aree a rischio reato potranno essere proposte al Consiglio di Amministrazione di Teleippica, sia dall'Organismo di Vigilanza che dagli altri organi di controllo della Società, per effetto dell'evoluzione dell'attività di impresa e conseguentemente di eventuali modifiche dell'attività svolta dalle singole Direzioni/Funzioni.

Nell'ambito di ciascuna **Area a Rischio Reato, gestita totalmente o parzialmente da Teleippica**, sono state individuate le c.d. "attività sensibili", ossia quelle attività al cui svolgimento è connesso il rischio di commissione dei reati in oggetto.

Sono state, inoltre, identificate le funzioni o i ruoli aziendali coinvolti nell'esecuzione di tali attività "sensibili". L'individuazione dei ruoli/funzioni non deve considerarsi, in ogni caso, tassativa atteso che ciascun soggetto aziendale potrebbe in linea teorica essere coinvolto.

Sono stati individuate, altresì, in via esemplificativa, con riferimento a ciascuna area, alcune potenziali modalità di realizzazione dei reati ed i controlli specifici a presidio dei rischi reato in oggetto.

Nella sezione 4.2 del presente documento, inoltre, sono stati identificati i Principi e regole particolari di comportamento a presidio dei rischi reato in oggetto.

3.1 Le Aree potenzialmente a Rischio Reato gestite parzialmente o totalmente da Teleippica. Le attività "sensibili", i ruoli aziendali coinvolti e le potenziali modalità di realizzazione dei reati

a) Gestione dei sistemi informativi

Attività sensibili:
- Acquisizione, sviluppo e manutenzione dei sistemi informatici;
- Installazione e utilizzo di programmi software;
- Gestione della configurazione delle componenti software ed hardware installate sulle postazioni di lavoro.

Processi e ruoli aziendali coinvolti:
- Gestione delle componenti software/hardware, delle reti aziendali, dei flussi informativi informatici e della custodia dei dati - Area ICT.

Possibili modalità di commissione del reato
A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui Teleippica acquisti una singola licenza *software* e provveda alla duplicazione del programma, in modo da distribuirlo illegalmente all'interno della propria organizzazione.

Presidi di controllo esistenti:
Per ciò che concerne la presente Area a Rischio e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.
In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:
- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei componenti software/hardware, delle reti aziendali, dei flussi informativi informatici e della custodia dei dati;
- Previsione, all'interno del Codice Etico, che tutti i rapporti con le Terze Parti siano ispirati a principi di lealtà, correttezza e onestà;
- Previsione di divieto di procedere all'installazione di qualsiasi software o hardware senza preventiva autorizzazione;
- L'utilizzo di dispositivi rimovibili (floppy disk, cd rom, cd riscrivibili, nastri magnetici, chiavi USB) può avvenire solo previa autorizzazione.

b) Gestione dei contenuti editoriali

Attività sensibili:

- Utilizzo e sfruttamento di materiale editoriale pubblicato presso i media (canali televisivi, radio, ecc.).

Processi e ruoli aziendali coinvolti:

- Pubblicazione di materiale editoriale - Area Editoriale.

Possibili modalità di commissione del reato

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui Teleippica provveda alla diffusione presso le proprie reti radio/televisive di un contenuto multimediale senza i necessari requisiti.

Presidi di controllo esistenti:

Per ciò che concerne la presente Area a Rischio e le attività sensibili relative, la Società ha predisposto una serie di punti di controllo volti a prevenire il rischio che siano commesse possibili violazioni.

In particolare, nello svolgimento delle loro mansioni i soggetti coinvolti nell'Area a Rischio devono rispettare i principi contenuti nel Modello (Parte Generale e Parte Speciale), nelle procedure, nel sistema di procure e deleghe e nel Codice Etico; in via esemplificativa e non esaustiva possono essere menzionati i seguenti controlli esistenti:

- Regolamentazione, tramite procedura, dei ruoli, delle attività, delle responsabilità e dei controlli connessi alla gestione dei contenuti editoriali;
- Verifica preventiva, in merito alla titolarità, da parte di Teleippica, dei diritti privatistici relativi ai contenuti editoriali da mettere in onda presso i media (canali radio-televisivi, ecc.);
- Autorizzazione dei contenuti editoriali da mettere in onda presso i media (canali radio-televisivi, ecc.);
- Reporting periodico in merito all'utilizzo di materiale editoriale relativo ad opere di ingegno altrui messo in onda presso i media (canali radio-televisivi, ecc.);
- Approvazione del Report SIAE, relativo agli importi da pagare sui diritti privatistici di opere di ingegno altrui utilizzati durante la messa in onda sui media (canali radio-televisivi, ecc.);
- Archiviazione di tutti i documenti relativi ai contenuti editoriali messi in onda sui media (canali radio-televisivi, ecc.).

4. I controlli aziendali

I Destinatari del Modello devono rispettare i principi e le regole di comportamento, generali e particolari, riportate di seguito.

4.1. Principi e regole generali di comportamento

Tutte le attività ricomprese nelle Aree a Rischio Reato devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure di Teleippica, nonché le regole contenute nel presente Modello.
Inoltre, ai Destinatari del Modello è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, considerati tali da integrare, in maniera diretta o indiretta, le fattispecie di reato di cui all'articolo 25-*novies* del D.Lgs. n. 231/01;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé Reati di Violazione del Diritto d'autore possano potenzialmente diventarlo.

4.2. Principi e regole particolari di comportamento

E' fatto divieto, in particolare, di:

- utilizzare e sfruttare materiale audio, video o fotografico su cui la Società non possa acquisire titolo di proprietà o licenza d'uso, ivi compreso, a titolo esemplificativo e non esaustivo, l'utilizzo di *materiale audio-visivo* contraffatto;
- utilizzare disegni, immagini o contenuti dell'ingegno coperti da diritto d'autore, senza le autorizzazioni previste dalla legge;
- installare ed utilizzare *software* e programmi non approvati dalla Società e non correlati all'attività professionale espletata dagli utilizzatori;
- installare ed utilizzare, sui sistemi informativi della Società, *software* mediante i quali è possibile scambiare ogni tipologia di file con altri soggetti all'interno dell'organizzazione, senza alcuna possibilità di controllo da parte della Società stessa;
- utilizzare *software* privi delle necessarie autorizzazioni/ licenze;
- duplicare e/o diffondere, in qualsiasi forma, programmi, *utilities*, archivi o *database* soggetti a tutela del diritto d'autore, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nel rispetto delle norme previste dalla legge;
- copiare CD, e più in generale supporti di memorizzazione, sottoposti a licenze d'uso, se non previa autorizzazione e nel rispetto delle norme previste dalla legge.

5. Compiti dell'OdV

Fermi restando i compiti e le funzioni dell'Organismo di Vigilanza statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati in Violazione del Diritto d'Autore, lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei Reati in violazione del diritto d'autore, previsti dal Decreto;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV svolge in piena autonomia le proprie attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici e/o a campione sulle attività connesse ai Reati in violazione del diritto d'autore al fine di verificare la corretta implementazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

L'OdV comunica risultati della propria attività di controllo relativamente ai Reati in violazione del diritto d'autore al Consiglio di Amministrazione e al Collegio Sindacale secondo le modalità definite dalla Parte Generale del Modello.

MODELLO
DI ORGANIZZAZIONE GESTIONE E CONTROLLO
D.LGS. 231/01

Parte Speciale F

PRINCIPI GENERALI DI CONDOTTA APPLICABILI ALLE ALTRE FAMIGLIE DI REATO RILEVANTI

Teleippica SRL

1. Premessa

La presente Parte Speciale costituisce parte integrante del Modello di cui Teleippica S.r.l. (di seguito, in breve anche "*Teleippica*" o "*Società*") si è dotata al fine di soddisfare le esigenze preventive di cui al D. Lgs. 231/01 (di seguito, in breve anche "*Decreto*").

Tutti i Destinatari del Modello, così come individuati nella Parte Generale del medesimo, sono chiamati all'osservanza dei principi generali di condotta di seguito indicati, nonché ad adottare, ciascuno in relazione alla funzione in concreto esercitata, comportamenti conformi ad ogni altra norma e/o procedura che regoli in qualsiasi modo le attività rientranti nell'ambito di applicazione del Decreto.

2. Principi generali di condotta applicabili alle altre famiglie di reato rilevanti

Come indicato nella Parte Generale del Modello, alla luce della specifica operatività di Teleippica, in relazione a: (i) *gli illeciti in materia di delitti di criminalità organizzata* (art. *24-ter* del Decreto); (ii) *i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio* (art. *25-octies* del Decreto); (iii) i *reati ambientali* (art. *25-undecies* del Decreto); (iv) il *delitto di impiego di cittadini di paesi terzi con soggiorno irregolare* (art. *25-duodecies* del Decreto), l'esito dell'attività di *risk assessment* ha portato a ritenere, sebbene applicabili e rilevanti, minore la concreta possibilità di commissione di tali reati, in virtù dell'attività svolta dalla Società e pertanto per essi trovano applicazione i principi generali di condotta di seguito descritti.

2.1 Delitti di Criminalità Organizzata di cui all'art. 24-ter del D.Lgs. 231/01

In considerazione della natura peculiare dei Delitti di Criminalità Organizzata che porta a ritenere ***diffuso*** e ***non localizzato*** a specifiche Aree Aziendali il rischio della loro commissione, indipendentemente dall'attività svolta dalla Società, avvalendosi del vincolo associativo, per l'individuazione delle Aree a Rischio e dei relativi presidi di controllo, volti a prevenire la commissione dei Delitti stessi, si rinvia a quanto contenuto nelle altre Parti Speciali del presente Modello.

Inoltre, ai Destinatari è fatto divieto di:

- porre in essere attività non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico;
- fornire, direttamente o indirettamente, fondi a favore di soggetti che intendono porre in essere uno o più reati associativi ovvero a favore di soggetti che perseguono, direttamente o in qualità di prestanome, finalità di criminalità organizzata, agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche;
- riconoscere compensi in favore di terzi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti;
- ricevere compensi per forniture o prestazioni inesistenti o che esulano dalla ordinaria attività d'impresa;
- erogare liberalità a favore di enti e soggetti vicini alla criminalità organizzata;
- assumere personale risultante vicino alla criminalità organizzata.

Ai fini dell'attuazione dei comportamenti di cui sopra vige l'obbligo di:

- verificare l'attendibilità commerciale e professionale dei fornitori e delle controparti contrattuali, nonché la loro onorabilità;
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- espletare i controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso Terzi e ai pagamenti derivanti da operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte, degli istituti di credito utilizzati e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- effettuare le opportune verifiche sui flussi di tesoreria;
- identificare la funzione aziendale responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità;
- adottare adeguati programmi di formazione del personale.

2.2. Delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio di cui all'art. 25-*octies* del D.Lgs. 231/01

Ai fini della commissione dei reati di cui all'art. 25-*octies* del D.Lgs. 231/01, presupposto comune e necessario è il trasferimento di beni, denaro o altre utilità di provenienza illecita.

Pertanto, le attività di *risk assessment* effettuate da Teleippica hanno evidenziato le "**Aree a Rischio Reato**" (anche totalmente o parzialmente esternalizzate) di seguito elencate:

- *Amministrazione del personale;*
- *Gestione dei contenziosi;*
- *Gestione degli omaggi, delle ospitalità e delle spese di rappresentanza;*
- *Amministrazione, contabilità e bilancio;*
- *Tesoreria;*
- *Gestione ciclo passivo;*
- *Contenuti editoriali.*

In particolare Destinatari è fatto divieto di:

- porre in essere condotte tali da integrare i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- porre in essere attività non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

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

- garantire il rispetto dei principi di correttezza, trasparenza e buona fede nell'ambito dei rapporti con i consulenti, i fornitori, i partner commerciali e, in genere, con le controparti contrattuali;
- richiedere tutte le informazioni necessarie al fine di accertare l'attendibilità commerciale/professionale dei fornitori e delle controparti in genere;
- garantire la corretta gestione della politica fiscale, anche con riguardo alle eventuali transazioni con i paesi di cui al DM 21 novembre 2001 e 23 gennaio 2002 e loro successive modifiche ed integrazioni;
- segnalare all'Organismo di Vigilanza eventuali irregolarità riscontrate in relazione ad eventi o circostanze che possono avere rilevanza in relazione alla commissione di reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.

Infine, con la finalità di attuare i comportamenti sopra descritti:

- è garantita l'esistenza di un sistema di deleghe con riferimento ai vincoli, ai limiti di spesa e alle responsabilità relativamente alle disposizioni di pagamento;
- sono identificati i ruoli e le responsabilità di autorizzazione, esecuzione e controllo dei pagamenti, con espressa indicazione dei soggetti chiamati ad eseguire le riconciliazioni bancarie;
- è prevista la segregazione dei compiti in modo da garantire la separazione delle attività tra soggetti deputati all'autorizzazione, all'esecuzione e al controllo;
- sono selezionati i professionisti e partner sulla base di criteri di trasparenza, di economicità e correttezza, garantendo la tracciabilità delle attività atte a comprovare i menzionati criteri;

- sono accertati i requisiti di onorabilità delle controparti e viene verificata la sussistenza di condanne penali o sanzioni a carico delle stesse;
- è attuata una costante formazione ed informazione degli esponenti aziendali sui temi relativi alla prevenzione dei fenomeni di riciclaggio;
- è fatto divieto di impiegare, sostituire o trasferire in attività economiche, finanziarie, imprenditoriali o speculative, denaro, beni o altre utilità provenienti da delitto non colposo oppure compiere, in relazione ad essi, altre operazioni in modo da ostacolare l'identificazione della provenienza delittuosa;
- sono resi edotti i Destinatari del Modello del dovere di segnalare all'OdV eventuali operazioni sospette o eventuali infrazioni delle regole comportamentali, sopra precisate, di cui siano venuti a conoscenza in occasione dell'attività professionale svolta.

2.3. Reati Ambientali di cui all'art. 25-undecies del D.Lgs. 231/01

Tutti coloro che operano per conto della Società sono tenuti al rispetto delle normative nazionali e internazionali in materia di tutela dell'ambiente, nonché dei regolamenti emessi dalle autorità competenti in materia ambientale.

A tutti coloro che operano per conto della Società è fatto divieto di:

- porre in essere condotte tali da integrare i reati ambientali, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione (ad esempio nell'ambito della gestione dei rifiuti, nella gestione degli scarichi, ecc.);
- porre in essere attività non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

In particolare, è tassativamente proibito qualsiasi comportamento finalizzato:

- all'instaurazione di rapporti con Terze Parti esterne che non abbiano adeguate caratteristiche tecnico-professionali o di correttezza o non dispongano di tutte le autorizzazioni ambientali necessarie allo svolgimento delle attività ad esse demandate, in nome o per conto della Società, con particolare riferimento alla raccolta, trasporto o smaltimento di rifiuti ed alla manutenzione degli impianti contenenti sostanze lesive dell'ozono;
- alla stipula o mantenimento di rapporti contrattuali (locazione, comodato, ecc.) con soggetti che si sappia o si abbia ragione di sospettare possano incorrere nella violazione delle norme ambientali;
- all'attività di gestione dei rifiuti (diretta o indiretta), in assenza delle necessarie autorizzazioni, con riferimento a tutte le fasi del ciclo di vita dei rifiuti (es. raccolta, trasporto, recupero, smaltimento, commercio, intermediazione, ecc.).

La Società ritiene inoltre importante integrare la gestione degli aspetti ambientali negli obiettivi di business per il mantenimento a lungo termine dei livelli di sostenibilità, redditività e competitività.

In tale ottica, la Società fissa i propri obiettivi ed i risultati da raggiungere sulla base delle seguenti principali attività:

- analisi degli aspetti e degli impatti ambientali connessi alle attività svolte ed ai servizi forniti dalla Società, al fine di rilevare le potenziali criticità ambientali e le conseguenti misure di prevenzione, protezione e mitigazione necessarie;
- monitoraggio del rispetto della normativa ambientale, anche con riferimento ai fornitori incaricati per lo svolgimento di servizi aventi potenziale rilevanza in merito alle tematiche ambientali;
- registrazione e controllo di evidenze volte a documentare l'attuazione e l'efficacia del monitoraggio e le azioni risolutive eventualmente implementate a valle dello stesso;
- formazione del personale sulle tematiche ambientali.

2.4. Delitto di impiego di cittadini di paesi terzi con soggiorno irregolare di cui all'art. 25-duodecies del D.Lgs. 231/01

In relazione a tale delitto, le attività di *risk assessment* effettuate da Teleippica hanno evidenziato le "**Aree a Rischio Reato**" (anche totalmente o parzialmente esternalizzate) di seguito elencate:

- *Selezione ed assunzione del personale.*
- *Amministrazione del personale;*
- *Gestione del Ciclo Passivo.*

A tutti coloro che operano per conto della Società è fatto divieto di:

- porre in essere condotte tali da integrare i reati di impiego di cittadini di paesi terzi con soggiorno irregolare, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- porre in essere attività non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

Inoltre con la finalità di attuare i comportamenti sopra descritti è previsto di:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare il Delitto di impiego di cittadini di paesi terzi con soggiorno irregolare;
- rispettare gli obblighi di legge in tema di lavoratori stranieri e permesso di soggiorno;
- considerare prevalente la tutela dei lavoratori ed il rispetto delle normative vigenti in materia rispetto a qualsiasi condizione economica;
- assicurare la verifica della regolarità del permesso di soggiorno in caso di assunzione di lavoratori stranieri ed un monitoraggio periodico finalizzato a verificare la validità/scadenza dei permessi di soggiorno stessi;
- in caso di lavori affidati a soggetti Terzi mediante appalti, viene sottoposta ad ogni fornitore una dichiarazione preventiva con cui lo stesso si impegna a non utilizzare, per l'espletamento delle attività oggetto del contratto, cittadini di paesi terzi con soggiorno irregolare, nonché a rispettare tutte le normative applicabili in tema di lavoro minorile e delle donne, condizioni igienico sanitarie, sicurezza e impiego di personale proveniente da paesi terzi;
- i contratti con le controparti contengono specifiche clausole che liberano Teleippica da qualsiasi responsabilità nel caso in cui la controparte utilizzi, per lo svolgimento delle prestazioni oggetto del contratto, cittadini di paesi terzi senza regolare permesso di soggiorno;
- assicurare la verifica preventiva circa la regolarità del permesso di soggiorno dei dipendenti degli appaltatori;
- vengono assicurati adeguati controlli preventivi sugli accessi fisici e segnalati tempestivamente ai responsabili competenti eventuali accessi da parte di soggetti sconosciuti o non identificati nell'ambito delle attività lavorative.

3. Controlli preventivi applicabili a tutte le Aree potenzialmente a Rischio Reato Diretto o Strumentali totalmente o parzialmente esternalizzate

Nell'espletamento delle proprie funzioni, oltre alle regole di condotte sopra indicate, i Destinatari devono conoscere e rispettare i presidi di controllo preventivi applicabili a tutte le Aree potenzialmente a Rischio Reato Diretto o Strumentali totalmente o parzialmente esternalizzate, di seguito elencati:

- formale definizione della politica per la esternalizzazione delle attività della Società, anche mediante individuazione dei metodi per la valutazione del livello delle prestazioni del fornitore (S.L.A.);
- formalizzazione di contratti di outsourcing nell'ambito dei quali è prevista:
  - l'identificazione dei servizi da erogare ed il relativo livello di servizio atteso (S.L.A.);
  - l'inserimento di clausole specifiche nell'ambito delle quali la società mandataria si impegna a rispettare i presidi di controllo previsti nel proprio Modello (ove adottato dalla società mandataria) nonché i principi ispiratori del Modello di Teleippica;
  - l'inserimento di clausole specifiche nell'ambito delle quali le società si impegnano, nei confronti l'una dell'altra, al rispetto più rigoroso dei propri Modelli (ove adottati), con particolare riguardo alle aree dei Modelli che presentano rilevanza ai fini delle attività gestite mediante contratto di *outsourcing* e della sua esecuzione; con tali clausole, si impegnano altresì a darsi reciprocamente notizia di eventuali violazioni, che dovessero verificarsi e che possano avere attinenza con il contratto e/o la sua esecuzione e più in generale, ad astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che possano integrare una qualsivoglia fattispecie di reato contemplata dal Decreto;
  - l'applicazione di sanzioni (ivi inclusa l'eventuale risoluzione del contratto) in caso di violazioni alle suddette prescrizioni.