MODELLO DI

ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL

DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

Approvato dal Consiglio di Amministrazione

nella seduta del 31 ottobre 2019

INDICE

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE

1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito "Decreto" o "D.Lgs. 231/01") ha introdotto nell'ordinamento italiano un regime di responsabilità, a carico di società ed associazioni con o senza personalità giuridica (di seguito denominate "Enti"), per alcuni reati commessi, nell'interesse o a vantaggio degli stessi, da:

- persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro funzione centrale e struttura operativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche, di fatto, la gestione e il controllo degli Enti medesimi;
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità della persona giuridica comporta l'applicazione di sanzioni che si aggiungono a quelle penali per la persona fisica che ha materialmente commesso il reato e sono entrambe, per quanto possibile, oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale.

L'elenco dei reati che danno luogo alla responsabilità dell'Ente è tassativamente previsto dalla legge e solo con legge può essere modificato. Alla data di approvazione del presente documento, è costituito dalle seguenti tipologie di condotte illecite richiamate espressamente nel Decreto:

- art. 24 (indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico);
- art. 24-*bis* (delitti informatici e trattamento illecito di dati);
- art. 24-*ter* (delitti di criminalità organizzata);
- art. 25 (concussione, induzione indebita a dare o promettere utilità e corruzione);
- art. 25-*bis* (falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento);
- art. 25-*bis*.1 (delitti contro l'industria e il commercio);
- art. 25-*ter* (reati societari);
- art. 25-*quater* (delitti con finalità di terrorismo o di eversione dell'ordine democratico);
- art. 25-*quater*.1 (pratiche di mutilazione degli organi genitali femminili);
- art. 25-*quinquies* (delitti contro la personalità individuale);
- art. 25-*sexies* (abusi di mercato);
- art. 25-*septies* (omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro);
- art. 25-*octies* (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio);
- art. 25-*novies* (delitti in materia di violazione del diritto d'autore);

- art. 25-*decies* (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria);
- art. 25-*undecies* (reati ambientali) e art. 256-*bis* D.Lgs. 152/2006 (combustione illecita di rifiuti);
- art. 25-*duodecies* (impiego di cittadini di Paesi terzi il cui soggiorno è irregolare);
- art. 25-*terdecies* (razzismo e xenofobia).

Altre fattispecie di reato potranno in futuro essere inserite dal legislatore nel Decreto Legislativo 231/01, con conseguente necessità di aggiornamento del presente Modello.

1.2. SANZIONI

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

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

In particolare, le sanzioni interdittive, di durata non inferiore a tre mesi e non superiore a due anni (fermo restando quanto previsto dall'art. 25 comma 5 del Decreto e fatti salvi i casi di interdizione definitiva richiamati dall'articolo 16 del Decreto) hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'Ente e sono costituite da:

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

Per i reati dell'art. 25 del Decreto che prevedono sanzioni interdittive, nei casi di condanna si applicano le stesse per una durata non inferiore a quattro anni e non superiore a sette anni, se il reato è stato commesso da un Soggetto Apicale e per una durata non inferiore a due anni e non superiore a quattro, se il reato è stato commesso da un soggetto subordinato. Se prima della sentenza di primo grado l'Ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e 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, tutte le sanzioni interdittive hanno la durata da tre mesi a due anni.

Le sanzioni interdittive sono applicate nelle ipotesi tassativamente indicate dal Decreto, solo se ricorre almeno una delle seguenti condizioni[1]:

1. 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 e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
2. in caso di reiterazione degli illeciti.

Il tipo e la durata delle sanzioni interdittive sono stabiliti dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'Ente e dell'attività svolta dallo stesso per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. In luogo dell'applicazione della sanzione, il giudice può disporre la prosecuzione dell'attività dell'Ente da parte di un commissario giudiziale.

Le sanzioni interdittive possono essere applicate all'Ente in via cautelare, quando sussistono gravi indizi per ritenere l'esistenza della responsabilità dell'Ente nella commissione del reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa natura di quello per cui si procede (art. 45 del Decreto). Anche in tale ipotesi, in luogo della misura cautelare interdittiva, il giudice può nominare un commissario giudiziale.

L'inosservanza delle sanzioni interdittive costituisce un reato autonomo previsto dal Decreto come fonte di possibile responsabilità amministrativa dell'Ente (art. 23 del Decreto).

Le sanzioni pecuniarie, applicabili a tutti gli illeciti, sono determinate attraverso un sistema basato su "*quote*" in numero non inferiore a cento e non superiore a mille e di importo variabile tra un minimo di Euro 258,23 ed un massimo di Euro 1.549,37. Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Oltre alle predette sanzioni, il Decreto prevede che venga sempre disposta (salvo per la parte che può essere restituita al danneggiato) la confisca del prezzo o del profitto del reato, che può avere ad oggetto anche beni o altre utilità dei valori equivalenti, mentre la pubblicazione della sentenza di condanna può essere disposta dal giudice in presenza di una sanzione interdittiva.

1.3. DELITTI TENTATI

L'Ente risponde anche degli illeciti dipendenti da delitti tentati. Nelle ipotesi di commissione nella forma del tentativo dei delitti indicati nel Capo I del Decreto, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. Si tratta di un'ipotesi particolare di c.d. "recesso attivo", previsto dall'art. 56, co. 4, c.p..

[1] Secondo quanto stabilito, con sentenza n. 42503 del 16 ottobre 2013, dalla Corte di Cassazione, sez. IV, il ricorrere di almeno una delle condizioni riportate non sarebbe necessario per i reati commessi con violazione della normativa sulla tutela della salute e sicurezza sul luogo di lavoro, per i quali dovrebbero comunque applicarsi tout court le sanzioni interdittive. La Corte di Cassazione ha infatti stabilito che, in caso di condanna dell'Ente per il delitto di lesioni personali gravi commesso con violazione della normativa suddetta (art. 590, c. 3, c.p.), le sanzioni interdittive devono essere applicate obbligatoriamente. Ciò, a parere di molti, sembrerebbe configurare un'ingiustificata disparità di trattamento sanzionatorio fra le ipotesi di reato previste dall'art. 25-septies del Decreto e tutti gli altri reati–presupposto della responsabilità amministrativa degli Enti.

1.4. REATI COMMESSI ALL'ESTERO

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere dei reati commessi all'estero, al fine di non lasciare sfornita di sanzione una condotta criminosa, nonché al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

I presupposti su cui si fonda la responsabilità dell'Ente per reati commessi all'estero sono:

a) il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;

b) l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;

c) l'Ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p..

Se sussistono i casi e le condizioni di cui ai predetti articoli del codice penale, l'Ente risponde, purché nei suoi confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

1.5. PROCEDIMENTO DI ACCERTAMENTO DELL'ILLECITO E SINDACATO DI IDONEITÀ DEL GIUDICE

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale e, per regola, è ispirata a ragioni di effettività, omogeneità ed economia processuale. Il processo nei confronti dell'Ente dovrà rimanere riunito, per quanto possibile, al processo penale instaurato nei confronti dell'autore del reato presupposto della responsabilità dell'Ente.

L'accertamento della responsabilità della società, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del reato presupposto per la responsabilità della società;
- l'accertamento in ordine alla sussistenza dell'interesse o vantaggio dell'Ente alla commissione del reato da parte del suo dipendente o apicale;
- il sindacato di idoneità sui modelli organizzativi adottati.

Il sindacato del giudice circa l'astratta idoneità del modello organizzativo a prevenire i reati di cui al Decreto è condotto secondo il criterio della c.d. "prognosi postuma". Il giudizio di idoneità è, cioè, formulato secondo un criterio sostanzialmente *ex ante*, per cui il giudice si colloca, idealmente, nella realtà aziendale nel momento in cui si è verificato l'illecito per saggiare la congruenza del modello adottato.

1.6. AZIONI ESIMENTI DALLA RESPONSABILITÀ

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità dell'Ente per i reati commessi nell'interesse o a vantaggio dello stesso, sia da soggetti apicali che da dipendenti.

Nel caso di reati commessi da soggetti in posizione apicale, l'art. 6 prevede l'esonero qualora l'Ente stesso dimostri che:

a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, gestione e controllo, nonché di proporne l'aggiornamento sia stato affidato ad un Organismo di Vigilanza dell'Ente, dotato di autonomi poteri di iniziativa e controllo;

c) le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il suddetto modello;

d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per quanto concerne i dipendenti non apicali, l'art. 7 prevede l'esonero nel caso in cui l'Ente abbia adottato ed efficacemente attuato prima della commissione del reato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il modello di organizzazione, gestione e controllo, deve rispondere alle seguenti caratteristiche:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo.

I modelli di organizzazione, gestione e controllo possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria (ad esempio Confindustria, che ha emanato per la prima volta le sue linee guida di tema di predisposizione del Modello ex D.Lgs. 231/01 il 7 marzo 2002 e successivamente ha provveduto nel tempo ad aggiornarle).

La predisposizione del presente Modello è ispirata alle *Linee Guida* emanate da Confindustria.

2. ADOZIONE DEL MODELLO DA PARTE DI TELECONSYS S.P.A.

2.1. OBIETTIVI E MISSION AZIENDALE

Teleconsys S.p.A. (di seguito "Teleconsys" o "Società") opera nel settore dell'informatica e delle telecomunicazioni con la missione di supportare le aziende e le organizzazioni pubbliche nel loro percorso di trasformazione digitale e di adozione di tecnologie innovative, fornendo attività di consulenza, di project management, di integrazione di sistemi e di prodotti propri o di terze parti, di sviluppo di moderne applicazioni software, di sicurezza informatica, di servizi gestiti, di ricerca e sviluppo, di open innovation, di formazione ed addestramento.

2.2. MODELLO DI GOVERNANCE

La *corporate governance* della Società, basata su un modello tradizionale, è così articolata:

- *Assemblea degli Azionisti*, competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla Legge e dallo Statuto;
- *Consiglio di Amministrazione*, investito dei più ampi poteri per l'amministrazione della Società, con facoltà di compiere tutti gli atti opportuni per il raggiungimento degli scopi sociali, ad esclusione di quelli riservati – dalla Legge e dallo Statuto – all'Assemblea degli Azionisti. Il Consiglio di Amministrazione (di seguito anche "C.d.A.") che ha delegato ad un suo componente i più ampi poteri di ordinaria e straordinaria amministrazione, conferendogli inoltre specifici poteri gestionali e bancari;
- *Collegio Sindacale*, cui spetta il compito di vigilare:
  - sull'osservanza della legge e dell'atto costitutivo nonché sul rispetto dei principi di corretta amministrazione;
  - sull'adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del sistema amministrativo contabile, anche in riferimento all'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione;
  - sull'adeguatezza delle disposizioni impartite alle società controllate in relazione alle informazioni da fornire per adempiere agli obblighi di comunicazione;
- *Società di revisione*, iscritta nell'albo tenuto dal Ministero dell'Economia e delle Finanze, incaricata dall'Assemblea degli Azionisti allo svolgimento dell'attività di revisione legale dei conti.

2.3. ASSETTO ORGANIZZATIVO E PARTECIPAZIONI

La struttura organizzativa della Società, ispirata all'attuazione di una separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, è stabilita con specifici Ordini di Servizio che definiscono formalmente sia l'Organigramma aziendale sia i ruoli, mission e responsabilità delle funzioni ed unità operative presenti nell'Organigramma stesso.

Tali documenti, resi noti a tutti i dipendenti della Società, assicurano la corretta individuazione degli ambiti di competenza di ciascuna struttura organizzativa all'interno dell'azienda.

La Società opera mediante un Sistema di Gestione Aziendale che soddisfa i requisiti delle seguenti norme internazionali per la Qualità:

- ISO 9001:2015;
- ISO 27001:2013.

Inoltre, Teleconsys è iscritta alla Sezione Speciale del Registro delle Imprese specificatamente dedicata alla "PMI Innovative" e detiene partecipazioni nella società Digital Innovation HUB del Lazio: Cicero HUB Scarl.

2.4. MOTIVAZIONI DELLA SOCIETÀ NELL'ADOZIONE DEL MODELLO

Teleconsys, al fine di assicurare che il comportamento di tutti coloro che operano per suo conto o nel suo interesse sia sempre conforme ai principi di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto opportuno procedere all'adozione di un Modello, in linea con le prescrizioni del Decreto e con le indicazioni della giurisprudenza in materia, nonché sulla base delle Linee Guida emanate da Confindustria.

Tale iniziativa è stata assunta nella convinzione che l'adozione di tale Modello - al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio - possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i coloro che operano nell'interesse o a vantaggio della Società, oltre che rappresentare una garanzia di affidabilità nelle relazioni con i partner commerciali/finanziari e essere un punto di forza nel "rating di legalità".

In particolare, si considerano ***destinatari*** del presente Modello e, come tali e nell'ambito delle specifiche competenze, tenuti alla sua conoscenza ed osservanza:

- i componenti del Consiglio di Amministrazione (CdA), nel fissare gli obiettivi, decidere le attività, realizzare i progetti, proporre gli investimenti e in ogni decisione o azione relativa all'andamento della Società;
- i componenti del Collegio Sindacale, nel controllo e nella verifica della correttezza formale e sostanziale dell'attività della Società e del funzionamento del sistema di controllo interno;
- l'Organismo di Vigilanza (O.d.V.), nell'assicurare il corretto svolgimento dei compiti assegnati dal presente Modello;
- l'Amministratore Delegato (AD), nel dare concretezza alle attività di direzione della Società, sia nella gestione delle attività interne che esterne;
- i dipendenti (dirigenti e non dirigenti) per lo svolgimento dell'attività, e tutti i collaboratori con cui si intrattengono rapporti contrattuali, a qualsiasi titolo, anche occasionali e/o soltanto temporanei assimilabili al lavoro dipendente (es. lavoratori somministrati, collaboratori a progetto, consulenti e professionisti che collaborano stabilmente con la Società, ecc.).

Inoltre, tutti coloro che intrattengono con la Società rapporti commerciali e/o finanziari di qualsiasi natura sono tenuti al rispetto, oltre che delle disposizioni contenute nel Decreto, anche dei principi stabiliti nel Codice Etico di Teleconsys, ovvero quelli del proprio Codice Etico, solo se ritenuti sostanzialmente analoghi ai fini della definizione delle regole di condotta da adottare.

2.4.1. FINALITÀ DEL MODELLO

Teleconsys – sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità morale e consapevole dell'importanza di adottare un efficace sistema di controllo nelle attività a rischio – a seguito dell'emanazione del Decreto, adotta il presente Modello di Organizzazione, Gestione e Controllo (di seguito "Modello"), impegnandosi altresì ad aggiornarlo ogni qualvolta dovesse essere necessario perché lo stesso rimanga adeguato a prevenire i rischi di commissione dei reati di cui al Decreto.

Il Modello si propone come finalità quelle di:

- migliorare il sistema di corporate governance della Società;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività della Società, con particolare riguardo ad impedire eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto di Teleconsys nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni normative, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti della Società;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse della Società, che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni fino alla risoluzione del rapporto contrattuale;
- ribadire che Teleconsys non tollera comportamenti illeciti, non rilevando in alcun modo la finalità perseguita ovvero l'erroneo convincimento di agire nell'interesse o a vantaggio della Società, in quanto tali comportamenti sono comunque contrari ai principi etici cui la Società si attiene e, quindi, in contrasto con il suo interesse e la sua cultura;
- censurare i comportamenti posti in essere in violazione del Modello attraverso la comminazione di sanzioni disciplinari e/o contrattuali.

2.4.2. IL PROCESSO DI PREDISPOSIZIONE DEL MODELLO

Il processo di predisposizione del Modello ha seguito diverse fasi che vengono qui di seguito descritte e che hanno portato, tra l'altro, all'elaborazione di un documento di *Risk Assessment* ex D.Lgs. 231/01.

1) *Mappatura delle attività a rischio*. Obiettivo di questa fase è stato l'analisi del contesto aziendale, al fine di mappare le aree di attività della Società e, tra queste, individuare quelle in cui possono essere realizzati i reati previsti dal Decreto. L'identificazione delle attività aziendali e delle aree a rischio è stata attuata attraverso il previo esame della documentazione aziendale (organigramma, procure, comunicazioni organizzative ed ordini di Servizio, procedure e "Schede Processo", ecc.) e la successiva effettuazione di interviste con i principali Referenti.
2) *Analisi dei rischi potenziali*. Con riferimento alla mappatura delle attività, effettuata nel particolare contesto in cui opera la Società ed alla relativa individuazione delle aree ed attività a rischio, sono stati identificati i reati potenzialmente realizzabili nell'ambito dell'attività aziendale, nonché le occasioni, le finalità e le modalità di commissione della condotta illecita. Tra le aree di attività a rischio sono considerate sia quelle che presentano un rilievo diretto come

attività che potrebbero integrare condotte di reato, sia quelle che possono avere un rilievo anche solo indiretto per la commissione di altri reati, risultando strumentali alla commissione degli stessi.

3) *As-is analysis*. Individuati i rischi potenziali, si è proceduto ad analizzare il sistema di controlli preventivi esistenti nei processi a rischio. In tale fase, si è provveduto alla rilevazione degli attuali presidi di controllo interno esistenti (procedure formali e/o prassi adottate, verificabilità, documentabilità o "tracciabilità" delle operazioni e dei controlli, separazione e segregazione delle funzioni, ecc.) mediante l'analisi della documentazione e le ulteriori informazioni fornite dalla Società avuto riguardo alle prassi in uso anche se non formalizzate.

4) *Gap analysis*. Sulla base dei risultati ottenuti nella fase precedente e del confronto con un modello teorico di riferimento (coerente con il Decreto, con le Linee Guida di Confindustria e con le migliori pratiche nazionali ed internazionali), la Società ha individuato una serie di aree di integrazione e/o miglioramento nel sistema dei controlli, a fronte delle quali sono state definite le opportune azioni da intraprendere.

5) *Predisposizione del Modello*. In considerazione degli esiti delle fasi sopra descritte, la Società ha provveduto alla predisposizione del Modello, la cui struttura è descritta nel successivo paragrafo 3.5.

Sulla base del *Risk Assessment* effettuato sono state individuate le attività a rischio di commissione di reati previsti dal D.Lgs. 231/01, riportate nella Parte Speciale del presente Modello.

Con riferimento a tutte le aree a rischio (anche quelle strumentali), sono stati altresì presi in esame gli eventuali rapporti indiretti, ossia quelli che la Società intrattiene, o potrebbe intrattenere, tramite soggetti terzi.

Nell'ambito delle attività di *Risk Assessment*, sono state analizzate le seguenti componenti del sistema di controllo preventivo:

- *Principi etici formalizzati*. Teleconsys ha provveduto a predisporre un Codice Etico, adottato con delibera del C.d.A., che esprime i propri valori etici e che definisce, con specifico riferimento alle attività a rischio reato, dei presidi generali di riferimento.
- *Sistema organizzativo*. La verifica dell'adeguatezza del sistema organizzativo si è basata sui seguenti criteri:
  - formalizzazione del sistema;
  - chiara definizione delle responsabilità attribuite e delle linee di dipendenza gerarchica;
  - esistenza della segregazione e contrapposizione di funzioni;
  - corrispondenza tra le attività effettivamente svolte e quanto previsto nelle comunicazioni organizzative e negli altri documenti della Società.
- *Sistema autorizzativo*. L'analisi ha riguardato l'esistenza di poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate e/o concretamente svolte. L'analisi è stata condotta sulla base dell'esame delle procure rilasciate e delle deleghe gestionali interne, alla luce dell'organigramma aziendale.

- *Procedure*. In tale ambito l'attenzione è stata rivolta alla verifica dell'esistenza di procedure formalizzate per regolamentare le attività svolte dalle strutture nelle aree a rischio, tenendo conto non soltanto delle fasi negoziali, ma anche di quelle di istruzione e formazione delle decisioni aziendali.
- *Sistema di controllo di gestione*. In tale ambito si è analizzato il sistema di controllo di gestione vigente nella Società, i soggetti coinvolti nel processo e la capacità del sistema di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare.
- *Monitoraggio e gestione della documentazione*. L'analisi ha riguardato l'esistenza di un idoneo sistema di monitoraggio dei processi per la verifica dei risultati e di eventuali non conformità, nonché l'esistenza di un idoneo sistema di gestione della documentazione tale da consentire la tracciabilità delle operazioni.
- *Sistema disciplinare*. Le analisi sono state finalizzate alla verifica dell'adeguatezza del sistema disciplinare vigente diretto a sanzionare l'eventuale violazione dei principi e delle disposizioni volte a prevenire la commissione dei reati, sia da parte dei dipendenti della Società sia da parte di Amministratori, Sindaci e collaboratori esterni.
- *Comunicazione al personale e sua formazione ed informazione agli altri Destinatari*. Le verifiche sono state rivolte ad accertare l'esistenza di forme di comunicazione e formazione per i Destinatari del Modello in materia di D.Lgs. 231/01.

2.5. STRUTTURA DEL DOCUMENTO

Il presente documento (Modello) è costituito da una "Parte Generale" e da una "Parte Speciale".

Nella "Parte Generale", dopo un richiamo ai principi del Decreto, alle linee Guida di Confindustria nonché alle motivazioni di adozione del Modello da parte della Società, vengono illustrate:

- le componenti essenziali del Modello;
- i principali aspetti inerenti l'O.d.V.;
- la formazione del personale e la diffusione del Modello nel contesto aziendale ed extra-aziendale;
- il sistema disciplinare e le misure da adottare in caso di mancata osservanza delle prescrizioni del modello stesso.

La "Parte Speciale" riporta i principi generali di comportamento e, per ogni area a rischio individuata in sede di *Risk Assessment*:

- la descrizione del potenziale profilo di rischio;
- le attività a rischio e gli enti coinvolti (Direzioni/Aree) nell'ambito della specifica area a rischio;
- i protocolli di controllo specifici.

2.6. ELEMENTI DEL MODELLO

Come sopra accennato, le componenti del sistema di controllo preventivo che devono essere attuate a livello aziendale per garantire l'efficacia del Modello sono:

- principi etici finalizzati alla prevenzione dei reati previsti dal Decreto;
- sistema organizzativo chiaro e adeguatamente formalizzato;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite;
- procedure operative, manuali od informatiche, volte a regolamentare le attività nelle aree aziendali a rischio con gli opportuni punti di controllo;
- sistema di controllo di gestione in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità;
- sistema di monitoraggio e di gestione della documentazione;
- sistema disciplinare adeguato a sanzionare la violazione delle norme del Codice Etico e delle altre indicazioni del Modello;
- sistema di comunicazione, all'interno ed all'esterno, e formazione del personale avente ad oggetto tutti gli elementi del Modello e del Codice Etico.

2.7. IL MODELLO ED IL CODICE ETICO

Il Codice Etico adottato da Teleconsys ha lo scopo di stabilire i principi di "deontologia aziendale" che la Società riconosce come propri, esplicitando i valori ai quali i dipendenti, gli Organi Sociali, i Consulenti ed i Partners devono adeguarsi, accettandone i principi e le regole di condotta previsti.

Il Codice Etico, pertanto, pur costituendo un documento distinto ed autonomo rispetto al presente Modello, può considerarsi ad esso complementare, in quanto diretto e destinato a creare, insieme a quest'ultimo, un "corpus" vincolante di regole di comportamento, volte alla prevenzione di condotte illecite nell'ambito dei comportamenti adottati dai Destinatari.

2.8. MODIFICHE ED INTEGRAZIONI DEL MODELLO

Il Modello è soggetto ad una continua attività di monitoraggio da parte dell'O.d.V. al fine di valutarne l'applicazione e l'efficacia. Eventuali carenze sono oggetto di attività di aggiornamento del Modello.

Gli interventi di adeguamento e/o aggiornamento del Modello sono espressamente prescritti dall'art. 6, co. 1, lett. b) del Decreto, e sono realizzati principalmente in occasione di:

- emanazione di nuove normative;
- violazioni del Modello e/o esiti negativi di verifiche sull'efficacia del medesimo;
- modifiche della struttura organizzativa o delle aree di business di Teleconsys.

Tali interventi sono orientati al mantenimento nel tempo dell'efficacia del Modello, e rivestono pertanto un'importanza prioritaria.

Resta comunque inteso che, i richiami alle strutture organizzative ed alle figure professionali effettuati nel Modello, in caso di modifiche interne dell'assetto aziendale e fino all'aggiornamento del Modello

stesso, si devono intendere effettuati alle nuove strutture ovvero alle nuove figure professionali che hanno assunto i compiti e le responsabilità di quelle qui indicate.

Tenuto conto che il presente Modello è un "atto di emanazione dell'organo dirigente", in conformità alle prescrizioni dell'art. 6, comma 1, lettera a del Decreto, la sua adozione, così come le successive modifiche ed integrazioni sono rimesse alla competenza del C.d.A., anche su proposta dell'O.d.V.. Modifiche od integrazioni, non sostanziali e di carattere formale, in conseguenza o meno di già avvenute delibere del C.d.A., possono essere direttamente recepite nel Modello a cura dell'Amministratore Delegato.

3. ORGANISMO DI VIGILANZA

3.1. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza (di seguito Organismo o "O.d.V.") è istituito ai sensi dell'art. 6, lettera b del Decreto in forma monocratica, composto da un membro esterno alla Società, scelto tra soggetti particolarmente qualificati e con esperienza nell'esercizio di attività professionali o di insegnamento universitario in materie giuridiche, economiche e finanziarie.

L'Organismo è nominato dal Consiglio di Amministrazione (di seguito anche CdA) che stabilisce così la durata in carica ed il compenso; l'O.d.V. resta in carica, in ogni caso, fino alla nomina del successore.

Tale Organismo potrà avvalersi, nello svolgimento dei propri compiti, della Funzione Internal Audit, di altre Direzioni e/o Funzioni di Teleconsys e/o di consulenti esterni che saranno ritenuti utili allo svolgimento delle proprie attività.

In particolare:

- l'autonomia ed indipendenza delle quali l'Organismo deve necessariamente disporre sono assicurate dalla presenza di un membro esterno alla Società, privo dunque di mansioni operative e di interessi che possano confliggere con l'incarico, condizionandone l'autonomia di giudizio e valutazione. Riporta direttamente al Consiglio di Amministrazione ed al Presidente. Le attività poste in essere dall'O.d.V. non possono essere sindacate da alcun altro organismo o struttura aziendale, fatto ovviamente salvo il potere-dovere del Consiglio di Amministrazione di vigilare sull'adeguatezza dell'intervento posto in essere. Inoltre, l'Organismo comunica al Consiglio di Amministrazione il budget occorrente, da impiegare per le spese necessarie all'esercizio delle funzioni che gli sono affidate;
- la professionalità è assicurata dalle specifiche competenze in materia, dovendosi individuare l'O.d.V. tra professionisti di comprovata competenza ed esperienza nelle tematiche giuridiche, economico o finanziarie; inoltre, è riconosciuta la facoltà all'Organismo di avvalersi, al fine dello svolgimento del suo incarico e con assoluta autonomia di budget, delle specifiche professionalità sia delle varie strutture organizzative aziendali sia di consulenti esterni;
- la continuità di azione è garantita dalla circostanza che l'Organismo opera in via continuativa all'attività di vigilanza sul Modello ed opera sistematicamente presso la Società per lo svolgimento dell'incarico assegnatogli.

L'O.d.V. è dotato:

- di un apposito Regolamento espressione della sua autonomia operativa e organizzativa, volto a disciplinare, in particolare, il funzionamento delle proprie attività;
- di "autonomi poteri di iniziativa e controllo" (cfr. art. 6 del Decreto) e, pertanto, gli sono garantite la necessaria autonomia ed indipendenza.

L'O.d.V. riferisce direttamente al Presidente ed al C.d.A. ed informa della sua attività il Collegio Sindacale.

La nomina quale membro dell'O.d.V. è condizionata, come detto, alla presenza di determinati requisiti professionali soggettivi, nonché all'assenza di cause di incompatibilità con la nomina stessa e di potenziali conflitti di interesse con il ruolo ed i compiti che andrebbe a svolgere. In tale contesto, costituiscono motivi di ineleggibilità dell'O.d.V.:

- avere rapporti di coniugio, parentela o di affinità entro il quarto grado con gli Amministratori e con i membri del Collegio Sindacale;
- intrattenere, direttamente o indirettamente, relazioni economiche e/o rapporti contrattuali, a titolo oneroso o gratuito, con Teleconsys, di rilevanza tale da condizionarne l'autonomia di giudizio;
- essere titolare, direttamente o indirettamente, di partecipazioni azionarie in Teleconsys o in Società partecipate o collegate tali da comprometterne l'indipendenza;
- trovarsi nella condizione giuridica di interdetto, inabilitato, fallito o condannato a una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi;
- essere stato sottoposto a misure di prevenzione disposte dall'autorità giudiziaria, salvi gli effetti della riabilitazione;
- essere sottoposti a procedimenti penali, condannati o soggetti a pena ai sensi degli artt. 444 e ss. c.p.p., salvi gli effetti della riabilitazione, in relazione ad uno dei reati previsti dal D.Lgs. 231/01;
- essere destinatari di un provvedimento di applicazione di una sanzione per uno dei reati di cui agli articoli 185 e 187-bis del TUF;
- essere colpito da cause di ineleggibilità ai sensi degli artt. 2399 lett. c e 2409-septiesdecies c.c..

La cessazione dalla carica può essere determinata da rinuncia, decadenza o revoca.

La rinuncia dell'Organismo può essere esercitata in qualsiasi momento e deve essere comunicata al C.d.A. e al Collegio Sindacale per iscritto.

La decadenza dell'Organismo è prevista:

- qualora vengano meno i requisiti precedentemente riportati, ovvero
- nel caso di grave infermità che lo renda inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, ne determini l'assenza per un periodo superiore a sei mesi.

In questi casi, il C.d.A., esperiti gli opportuni accertamenti, sentito l'interessato, stabilisce un termine non inferiore a 30 giorni entro il quale deve cessare la situazione di decadenza. Trascorso tale termine senza che la predetta situazione sia cessata, deve dichiararne l'avvenuta decadenza.

Al fine di garantire la necessaria stabilità dell'O.d.V. e di tutelarne il legittimo svolgimento delle funzioni da una rimozione ingiustificata, la revoca dei poteri propri dell'O.d.V. e l'attribuzione di tali poteri ad altro soggetto, potrà avvenire soltanto per giusta causa, con apposita delibera del Consiglio di Amministrazione, sentito il Collegio Sindacale.

A tale proposito, per "giusta causa" di revoca dell'O.d.V devono intendersi:

- un grave inadempimento dei propri doveri così come definiti nel presente Modello;
- una sentenza di condanna o di patteggiamento emessa nei suoi confronti per aver commesso illeciti previsti dal Decreto;

- un provvedimento di condanna della Società per uno degli illeciti previsti dal Decreto, ove risulti l'"omessa o insufficiente vigilanza" da parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- la violazione degli obblighi di riservatezza cui è tenuto l'O.d.V. in ordine alle notizie ed informazioni acquisite nell'esercizio delle sue funzioni, fatti salvi gli obblighi di informazione espressamente previsti dal presente Modello. In particolare, l'Organismo deve assicurare la riservatezza delle informazioni di cui viene in possesso - con particolare riferimento alle segnalazioni che dovessero pervenire in ordine a presunte violazioni del Modello – ed astenersi dal ricercare ed utilizzare informazioni riservate, per fini diversi da quelli indicati dall'art. 6 del Decreto. In ogni caso, ogni informazione in possesso dell'Organismo deve essere trattata in conformità con la legislazione vigente in materia e, in particolare, in conformità con le norme sulla privacy.

Qualora la revoca venga esercitata, il Consiglio di Amministrazione provvederà senza indugio alla nomina di un nuovo e diverso Organismo.

Ove sussistano gravi ragioni di convenienza, il Consiglio di Amministrazione, sentito il Collegio Sindacale, potrà disporre la sospensione dalle funzioni dell'O.d.V., provvedendo tempestivamente alla nomina di un nuovo Organismo *ad interim*.

In caso di rinuncia, decadenza o revoca dell'Organismo, il Consiglio di Amministrazione deve provvedere senza indugio alla sua sostituzione.

3.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA

Il ruolo dell'O.d.V. della Società consiste:

- nella verifica e vigilanza sul rispetto del Modello;
- nel segnalare eventuali necessità di aggiornamento del Modello;
- nel monitorare l'effettuazione di un'adeguata attività di informazione e formazione sullo stesso.

Più in particolare è compito dell'O.d.V.:

- monitorare la validità nel tempo del Modello, promuovendo, anche previa consultazione delle Direzioni/Funzioni aziendali interessate, le azioni necessarie per assicurarne l'efficacia. Tale compito comprende la formulazione di proposte di adeguamento (ad esempio con riferimento alle procedure in essere, al sistema dei poteri, ecc.) da inoltrare al Vertice e di verificarne l'attuazione e la funzionalità;
- verificare l'efficacia del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati di cui al Decreto, proponendone, se ritenuto opportuno, eventuali aggiornamenti;
- effettuare la verifica del corretto svolgimento presso le Direzioni/Funzioni aziendali ritenute a rischio di reato delle attività sociali, in conformità al Modello adottato;
- effettuare una verifica degli atti compiuti dai soggetti dotati di poteri di firma e dei poteri autorizzativi e di firma esistenti, per accertarne la coerenza con le loro responsabilità organizzative e gestionali e proporre il loro aggiornamento e/o modifica ove necessario.

Inoltre, è compito dell'O.d.V.:

- definire i flussi informativi che gli consentano di essere periodicamente aggiornato dalle Direzioni/Funzioni aziendali interessate sulle attività valutate a rischio di reato, nonché stabilire modalità di comunicazione, al fine di acquisire conoscenza delle eventuali violazioni del Modello;
- attuare, in conformità al Modello, un efficace flusso informativo nei confronti del C.d.A. che consenta all'Organismo di riferire sull'efficacia e sull'osservanza dello stesso;
- promuovere, di concerto con le competenti Direzioni/Funzioni aziendali un adeguato processo formativo del personale con idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e delle procedure aziendali;
- promuovere e coordinare le iniziative volte ad agevolare la conoscenza del Codice Etico da parte di tutti coloro che operano per conto della Società.

Per lo svolgimento degli adempimenti sopra elencati, all'O.d.V. sono attribuiti i poteri di seguito indicati:

- accedere ad ogni documento e/o informazione aziendale ai fini dello svolgimento delle funzioni attribuitegli;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di competenza, osservando quanto previsto dalla Società per l'assegnazione di tali incarichi;
- richiedere alle Direzioni/Funzioni le informazioni, i dati e le notizie necessarie all'espletamento dei propri compiti ed assicurarsi risposte tempestive;
- procedere, qualora si renda necessario, all'audizione diretta dei dipendenti e degli amministratori della Società;
- richiedere informazioni a fornitori, consulenti esterni, partner commerciali e revisori.

L'O.d.V., infine, è dotato dal C.d.A. di poteri di spesa adeguati. Tali poteri, potranno essere impiegati per acquisire consulenze professionali, strumenti e/o quant'altro si rendesse necessario od opportuno per lo svolgimento delle funzioni proprie dell'O.d.V., secondo le modalità e nel rispetto delle procedure di acquisto adottate dalla Società.

3.3. INFORMATIVA DELL'ORGANISMO DI VIGILANZA NEI CONFRONTI DEGLI ORGANI SOCIALI

In merito all'attività di reporting, l'O.d.V. provvede a fornire un'informativa scritta almeno annuale nei confronti del C.d.A. con riferimento ai seguenti principali aspetti:

- l'attività complessivamente svolta nel periodo, con specifica descrizione delle verifiche effettuate;
- le criticità emerse sia in termini di comportamenti o eventi interni alla Società, sia in termini di efficacia del Modello;
- le segnalazioni di infrazioni del Modello ricevute nel corso del periodo e le azioni intraprese dall'O.d.V. stesso e dagli altri soggetti interessati a fronte di tali segnalazioni;
- le attività cui non si è potuto procedere per giustificate ragioni di tempo e/o risorse;

- i necessari e/o opportuni interventi correttivi e migliorativi del Modello ed il loro stato di attuazione;
- lo stato dell'attuazione del Modello della Società;
- il Piano di attività per il periodo successivo.

L'O.d.V. dovrà invece riferire tempestivamente al Presidente del C.d.A., e per conoscenza agli altri Consiglieri, in merito a:

- violazioni rilevanti del Modello ritenute fondate, di cui sia venuto a conoscenza per segnalazioni pervenute o che abbia accertato l'Organismo stesso;
- carenze organizzative o procedurali idonee a determinare il concreto pericolo di commissione di reati rilevanti ai fini del Decreto;
- modifiche normative particolarmente rilevanti ai fini dell'attuazione ed efficacia del Modello;
- mancata collaborazione da parte delle Direzioni/Funzioni aziendali (ad esempio rifiuto di fornire all'Organismo documentazione o dati richiesti, ovvero ostacolo alla sua attività, determinato anche da ritardi e/o negazione di comportamenti dovuti in base al Modello);
- ogni altra informazione ritenuta utile ai fini dell'assunzione di determinazioni da parte del Presidente del Consiglio di Amministrazione.

L'O.d.V. inoltre dovrà riferire senza indugio al Collegio Sindacale eventuali violazioni del Modello poste in essere dal Consiglio di Amministrazione o dalla società di revisione.

3.4. SEGNALAZIONI E FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

L'art. 6, comma 2, lett d) del Decreto impone la previsione nel modello di organizzazione, gestione e controllo di obblighi informativi nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza del modello stesso.

L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto stesso, nonché allo scopo di conferire maggiore autorevolezza alle richieste di documentazione necessarie all'Organismo nel corso delle sue verifiche.

3.4.1. SEGNALAZIONI DI PRESUNTE CONDOTTE ILLECITE

L'art. 6, comma 2 bis, del Decreto, impone che il Modello preveda "uno o più canali" che consentano ai Destinatari, tutelandone la riservatezza dell'identità, di presentare "segnalazioni circostanziate di condotte illecite" (c.d. "whistleblowing") e stabilisce forme di tutela per il segnalante.

Pertanto, ritenendo utile ampliare i requisiti "minimi" previsti dalla norma in relazione al "whistleblowing", è stabilito che i Destinatari del Modello sono tenuti a segnalare all'Organismo ogni informazione, di qualsiasi tipo, concernente la possibile commissione di reati o, comunque, la violazione del Modello o, in generale, le circostanze da cui possa emergere una carenza organizzativa o procedurale ovvero una necessità di adeguamento del Modello.

Pertanto, tutti i Destinatari del Modello sono tenuti a segnalare all'O.d.V. ogni informazione proveniente anche da terzi, di cui siano venuti a diretta conoscenza ed attinente alla violazione del Modello nelle aree di attività a rischio o ad eventuali altre irregolarità rilevanti ai sensi del Decreto e segnatamente le attività che siano o possano essere:

- contrarie ai principi contenuti nel Modello o nel Codice Etico adottato da Teleconsys;
- in violazione delle regole interne (quali le procedure aziendali, il sistema dei poteri e procure, i protocolli di controllo adottati in attuazione del Modello, ecc.) e che presentino profili di rischio tali da indurre a ravvisare il ragionevole pericolo di commissione di reati,
- dirette al compimento di uno o più reati.

È possibile inviare le segnalazioni all'O.d.V. secondo le seguenti modalità:

- comunicazione a mezzo casella di posta elettronica dedicata: odv@teleconsys.it;
- comunicazione scritta indirizzata a "Organismo di Vigilanza di Teleconsys S.p.A." presso la sede della Società (Teleconsys S.p.A. - Via Groenlandia, 31 – 00144 Roma).

L'O.d.V. e/o il personale della Società che ricevono segnalazioni e/o che sono interessate alla loro "gestione", sono tenuti a garantire l'assoluta riservatezza sui soggetti e sui fatti segnalati, utilizzando, a tal fine, criteri e modalità di comunicazione idonei a tutelare l'onorabilità delle persone menzionate nelle segnalazioni, nonché, ove possibile, l'anonimato dei segnalanti, affinché non possano essere oggetto di eventuali ritorsioni e, più in particolare, la Società:

- tutela coloro che effettuano segnalazioni in buona fede, da ritorsioni, discriminazioni o penalizzazioni, dirette o indirette, per motivi collegati alla segnalazione;
- vieta atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- garantisce la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede;
- garantisce che il personale sia a conoscenza delle procedure di segnalazione e sia in grado di usarle, essendo consapevole dei propri diritti e delle tutele nel quadro delle procedure adottate, mediante idonea comunicazione e formazione secondo le modalità previste nel capitolo 4;
- provvede, in caso di riscontrata violazione delle misure di tutela del segnalante, nonché di segnalazioni infondate rivelate con dolo o colpa grave, ad identificare ed applicare la sanzione ritenuta più adeguata alla circostanza, in accordo con quanto definito successivo capitolo 5.

La gestione delle segnalazioni e l'eventuale irrogazione di sanzioni disciplinari a seguito di tali segnalazioni, è effettuata dalla Società in coerenza e nel rispetto delle indicazioni della L. 179/17 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".

3.4.2. FLUSSI INFORMATIVI ORDINARI VERSO L'O.D.V.

Oltre le segnalazioni di cui al precedente paragrafo, l'O.d.V. riceve le seguenti informazioni, elencate a titolo esemplificativo e non esaustivo in relazione alle quali è opportuna un'informativa immediata, quali ad esempio:

- i provvedimenti notificati dall'Autorità Giudiziaria alla Società o ai suoi Amministratori, Dirigenti o dipendenti dai quali si evinca lo svolgimento di indagini condotte dalla medesima Autorità per illeciti di cui al D.Lgs. 231/01;
- le richieste di assistenza legale inoltrate dai Dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- l'evidenza dei procedimenti disciplinari svolti per violazioni del Modello, dei relativi esiti e motivazioni e delle eventuali sanzioni irrogate;
- ogni eventuale anomalia o irregolarità riscontrata nell'attività di verifica svolta dalla Funzione Internal Audit;
- eventuali infortuni sul luogo di lavoro, ovvero provvedimenti assunti dall'Autorità Giudiziaria o da altre Autorità in merito alla materia della sicurezza e salute sul lavoro;
- eventuali provvedimenti assunti dall'Autorità Giudiziaria o da altre Autorità in materia di ambiente, dai quali risulti una attuale o potenziale violazione delle norme in materia ambientale e/o delle autorizzazioni che disciplinano l'attività aziendale;
- le modifiche che intervengano in relazione alla struttura organizzativa di Teleconsys e del sistema delle deleghe adottato dalla Società;
- le eventuali erogazioni concesse, a qualunque titolo, a favore di Enti pubblici o soggetti che svolgano pubbliche funzioni;
- l'attività di informazione e formazione svolta in attuazione del Modello e la partecipazione alla medesima da parte del personale;
- la specifica reportistica a fronte delle diverse aree di attività a rischio, come indicato nel Modello e nelle specifiche procedure aziendali.

L'Organismo, per lo svolgimento dei propri compiti ha la facoltà - senza necessità di alcun consenso preventivo – di:

- chiedere ogni ulteriore documentazione o informazione che ritenesse utile;
- accedere presso tutte le Funzioni della Società.

Le informazioni sono trasmesse all'Organismo secondo le medesime modalità previste per effettuare le segnalazioni.

3.4.3. RACCOLTA, CONSERVAZIONE E ACCESSO ALL'ARCHIVIO DELL'O.D.V.

La documentazione raccolta e prodotta nel corso dello svolgimento della propria attività è conservata dall'O.d.V. in un proprio archivio. L'accesso a tale archivio è consentito, oltre all'O.d.V., solo a soggetti formalmente delegati ed autorizzati da quest'ultimo.

4. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO

4.1. FORMAZIONE DEL PERSONALE

La Società promuove la conoscenza del Modello, del Codice Etico e delle procedure aziendali tra tutti i Destinatari che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e a contribuire alla loro attuazione.

La Società, in cooperazione con l'O.d.V., gestisce la formazione del personale sui contenuti del D.Lgs. 231/01 e sull'attuazione del Modello attraverso uno specifico piano.

Il percorso di formazione indirizzato al personale direttivo e ai dipendenti della Società prevede seminari formativi in aula ovvero soluzioni in modalità "e-learning" su supporto informatico; la partecipazione alle sessioni di formazione è obbligatoria.

La Società assicura la tracciabilità e le evidenze documentali della partecipazione dei dipendenti alla formazione sulle disposizioni del Decreto e sul Modello.

Eventuali sessioni formative di aggiornamento saranno effettuate in caso di rilevanti modifiche apportate al Modello, al Codice Etico o relative a sopravvenute novità normative rilevanti per l'attività della Società, ove l'O.d.V. non ritenga sufficiente, in ragione della complessità della tematica, la semplice diffusione della modifica con le modalità descritte nel successivo paragrafo 4.2.

Ai neoassunti, nell'ambito del processo di inserimento nella Società, verrà effettuata una specifica formazione sul: Modello, Codice Etico e sistema procedurale.

4.2. INFORMATIVA AL PERSONALE

La Società provvede a dare al personale un'adeguata informativa in merito a:

- novità normative in materia di responsabilità amministrativa degli Enti;
- modifiche procedurali ed organizzative.

Per garantire tale informativa, la Società cura:

- la distribuzione, in modalità digitale, del Modello e del Codice Etico a tutto il personale in forza ed ai nuovi assunti al momento dell'assunzione;
- l'invio di e-mail o comunicazioni di aggiornamento sulle modifiche apportate al Modello, al Codice Etico ed alle Procedure aziendali, oltre che a quelle normative e/o organizzative rilevanti ai fini del Decreto.

4.3. INFORMATIVA A COLLABORATORI ESTERNI E PARTNER

La Società promuove la conoscenza e l'osservanza delle linee di condotta del Modello e del Codice Etico anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo ed i fornitori della Società.

L'informativa avviene, per tali soggetti, tramite la comunicazione dell'esistenza della parte Generale del Modello e del Codice Etico, con invito alla consultazione sul sito internet della Società.

Per quel che riguarda il Codice Etico, è responsabilità del Purchaising e General Affairs ovvero di eventuali altre strutture aziendali che gestiscono il rapporto contrattuale con i fornitori o consulenti terzi, ottenere l'adesione al medesimo da parte degli stessi, ovvero la conferma dell'adozione di un proprio Codice Etico (che presenti principi analoghi a quello di Teleconsys). Eventuali eccezioni (es. fornitori internazionali, ecc.) devono essere motivate e portate all'attenzione dell'O.d.V. Analoga procedura va osservata nei rapporti con partner commerciali o in occasione di accordi di ricerca e sviluppo.

La Società, inoltre, provvede ad inserire nei contratti con le controparti sopra menzionate apposite clausole contrattuali che prevedono, in caso di comportamenti non in linea con i principi etici della Società, opportune sanzioni sino alla risoluzione degli obblighi contrattuali. Anche in questo caso eventuali eccezioni devono essere motivate e portate all'attenzione dell'O.d.V.

5. SISTEMA DISCIPLINARE

5.1. PRINCIPI GENERALI

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'effettività del Modello stesso.

Al riguardo, infatti, l'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del Decreto stabiliscono che l'esonero da responsabilità dell'ente è subordinato, tra l'altro, alla prova dell'avvenuta introduzione di "*un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*".

La definizione di un sistema di sanzioni commisurate alla gravità della violazione e con finalità deterrenti concorre a rendere efficace l'azione di vigilanza dell'O.d.V. ed a garantire l'effettiva osservanza del Modello.

Nel rispetto di quanto previsto dal presente Sistema Disciplinare, nonché dalla legislazione vigente, dal CCNL e degli accordi contrattuali con le terze parti, le sanzioni saranno determinate tenendo conto dei principi di proporzionalità e di adeguatezza delle stesse rispetto alla gravità delle violazioni contestate. A tal fine, saranno considerati i seguenti fattori:

- la tipologia della violazione;
- la gravità della violazione;
- il grado di negligenza, imprudenza o imperizia dimostrate, tenuto anche conto della prevedibilità dell'evento;
- la responsabilità connessa alla posizione;
- la reiterazione della violazione;
- l'entità dell'eventuale danno, o dell'eventuale pericolo per la Società quale conseguenza diretta della violazione;
- il comportamento complessivo dell'autore della violazione, con particolare riguardo all'intenzionalità della condotta ed alle modalità di realizzazione della stessa;
- l'eventuale commissione, da parte dell'autore, di ulteriori violazioni del Modello, anche di differente natura, nei precedenti anni;
- l'eventuale sussistenza di più violazioni attuate con la medesima condotta;
- il concorso di più soggetti nella commissione della violazione.

L'applicazione del sistema disciplinare e delle relative sanzioni:

- è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'Autorità Giudiziaria a carico dell'autore materiale della condotta criminosa;
- non pregiudica in ogni caso il diritto della Società di agire nei confronti del soggetto responsabile al fine di ottenere il risarcimento di tutti i danni patiti a causa o in conseguenza della condotta accertata.

Ai fini del presente sistema disciplinare, e nel rispetto delle previsioni di cui alla contrattazione collettiva, laddove applicabili, costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del Modello, ivi compreso il mancato rispetto delle procedure aziendali, con

particolare riferimento a quelle evidenziate nella Parte Speciale, nonché la violazione delle misure di tutela del segnalante e/o l'effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate.

L'applicazione delle sanzioni disciplinari prescinde dall'avvio e/o dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dalla Società in piena autonomia ed indipendentemente dalla tipologia di illecito.

5.2. SANZIONI PER I CONSIGLIERI DI AMMINISTRAZIONE

I provvedimenti sanzionatori nei confronti degli Amministratori, commisurati alla gravità dell'infrazione commessa, che potranno essere deliberati dai competenti organi, sono i seguenti:

- la diffida al puntuale rispetto del Modello e/o del Codice Etico;
- il formale biasimo;
- la revoca totale o parziale delle deleghe conferite;
- la revoca ex art. 2383 comma 3 c.c..

5.3. LE SANZIONI PER I DIPENDENTI CON QUALIFICA DI DIRIGENTE

L'inosservanza delle norme indicate nel Modello, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte dei Dirigenti il cui rapporto di lavoro sia regolato dal vigente C.C.N.L. (di seguito "C.C.N.L. Dirigenti"), determinano l'applicazione delle seguenti misure sanzionatorie, fermo restando il rispetto delle procedure previste dall'art. 7 della legge 300/1970 ("Statuto dei lavoratori").

Più in particolare, il dirigente incorrerà nel:

- richiamo verbale;
- biasimo formale.

Nei confronti dei Dirigenti è altresì applicabile il ricorso al licenziamento, in conformità al CCNL, laddove la Società sia incorsa – per effetto della loro condotta secondo un nesso di causalità diretta – nelle sanzioni di cui al D.Lgs. n. 231/01 ovvero, in via preventiva, laddove la condotta tenuta dal Dirigente abbia assunto modalità antigiuridiche incompatibili con il mantenimento del rapporto di fiducia con la Società medesima.

Resta ferma la facoltà della Società di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del Giudice delle misure previste dal Decreto.

5.4. LE SANZIONI PER I DIPENDENTI NON AVENTI QUALIFICA DI DIRIGENTE

Nei confronti dei dipendenti non aventi la qualifica dirigenziale troveranno applicazione le sanzioni previste dal presente Sistema Disciplinare, nel rispetto della contrattazione collettiva applicabile ai diversi rapporti di lavoro, in relazione alle rispettive categorie di appartenenza.

Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori dipendenti, le stesse rientrano tra quelle previste dal contratto di lavoro, nel rispetto delle procedure previste dall'articolo 7 dello Statuto

dei Lavoratori (Legge n. 300 del 1970) e di eventuali normative speciali applicabili. In particolare, si prevede che il lavoratore che adotti un comportamento non conforme o violi le norme di condotta previste dal Modello, dal Codice Etico nonché da tutte le disposizioni interne adottate in attuazione dello stesso, incorrerà nei provvedimenti di:

- biasimo inflitto verbalmente per mancanze lievi;
- biasimo inflitto per iscritto nei casi di recidiva delle infrazioni di cui sopra;
- multa in misura non eccedente l'importo stabilito dal CCNL, per i casi previsti nel CCNL medesimo;
- sospensione dalla retribuzione e dal servizio, per i casi previsti nel CCNL e secondo le modalità in esso stabilite;
- licenziamento senza preavviso per i casi previsti nel C.C.N.L nonché per quanto specificato nell'ultimo capoverso del presente paragrafo.

In relazione ai lavoratori somministrati, qualora presenti, Teleconsys segnalerà la circostanza alla Società di Somministrazione, affinché la stessa applichi le sanzioni previste, dal suo sistema disciplinare interno e/o dalla contrattazione collettiva riferita ai diversi rapporti di lavoro, in relazione alle rispettive categorie di appartenenza.

In caso di gravi violazioni, Teleconsys potrà richiedere alla Società di Somministrazione l'allontanamento del lavoratore dalla sede di lavoro e l'eventuale interruzione del rapporto con la stessa Società di Somministrazione.

Resta inteso che il licenziamento è applicabile solo con riferimento a dipendenti la cui condotta abbia dato origine, a carico della Società, e secondo un nesso di causalità diretta, all'applicazione di sanzioni di cui al D.Lgs. n. 231/01 da parte dell'autorità giudiziaria.

5.5. LE SANZIONI PER I "TERZI DESTINATARI"

Nei confronti dei soggetti Terzi Destinatari (es. consulenti, collaboratori, fornitori, etc), grazie all'attivazione di opportune clausole contrattuali, potranno trovare applicazione le seguenti sanzioni:

- la diffida al puntuale rispetto del Codice Etico e dei principi contenuti nel Modello;
- la risoluzione del rapporto negoziale intercorrente con la Società.

A tal fine, nell'ambito dei rapporti con i Terzi Destinatari, Teleconsys inserirà appositi presidi volti a tutelare la Società in caso di violazioni delle norme presenti nel Codice Etico e nel Modello. Nelle lettere di incarico e/o negli accordi negoziali con detti terzi, la Società stabilirà apposite clausole volte a prevedere, in caso di violazioni accertate, l'applicazione delle misure sopra indicate.

5.6. LE SANZIONI PER I SINDACI

In caso di violazione del Modello e/o del Codice Etico da parte di uno o più Sindaci (o dell'intero Collegio Sindacale), i provvedimenti sanzionatori, commisurati alla gravità dell'infrazione commessa, che potranno essere deliberati dai competenti organi, sono i seguenti:

- la diffida al puntuale rispetto del Modello e/o del Codice Etico;

- il formale biasimo;
- la revoca del Collegio Sindacale ex art. 2400 c.c..

5.7. LE SANZIONI PER L'ORGANISMO DI VIGILANZA

In caso di violazione del Modello e/o del Codice Etico da parte dell'Organismo di Vigilanza, i provvedimenti sanzionatori, commisurati alla gravità dell'infrazione commessa, che potranno essere deliberati dal CdA, sono i seguenti:

- la diffida al puntuale rispetto del Modello e/o del Codice Etico;
- il formale biasimo;
- la revoca dell'incarico.

5.8. I COMPORTAMENTI SANZIONABILI E L'ACCERTAMENTO DELLE VIOLAZIONI

Fermi restando gli obblighi nascenti dalla Legge n. 300 del 1970 (c.d. "Statuto dei Lavoratori") e dalle altre norme di legge applicabili, i comportamenti sanzionabili che costituiscono violazione del Modello, a titolo esemplificativo e non esaustivo, possono essere individuati come segue:

- la violazione del Sistema dei Poteri e delle prescrizioni del Modello, nonché, se rilevante ai sensi del D.Lgs. 231/2001, la violazione delle disposizioni e dei protocolli di controllo interno, eventualmente adottati in attuazione dello stesso, delle procedure e dei regolamenti aziendali;
- il compimento di uno o più reati, rilevanti ai sensi del D.Lgs. 231/2001;
- la violazione degli obblighi di comunicazione delle informazioni o di segnalazione di presunte violazioni verso l'Organismo di Vigilanza, se rilevante ai sensi del D.Lgs. 231/2001.

Inoltre, ai sensi e per gli effetti di quanto stabilito dall'art. 6, comma 2 bis, lettera d) del Decreto, sono soggetti a sanzione coloro che:

- violino le misure di tutela del segnalante ovvero adottino o solo minaccino di adottare ritorsioni contro coloro che riferiscono presunte violazioni;
- effettuino, con dolo o colpa grave, segnalazioni di presunte violazioni che si siano rivelate infondate.

La Società vigila affinché nessuna ritorsione o misura discriminatoria sia adottata nei confronti dei soggetti segnalanti.

L'O.d.V., per tutte le segnalazioni ricevute, comprese quelle anonime, si attiverà tempestivamente al fine di svolgere, nei limiti delle proprie prerogative e dei propri poteri, un'analisi per valutare le seguenti alternative:

a) *procedere all'archiviazione* delle segnalazioni generiche o non sufficientemente circostanziate, di quelle palesemente infondate, nonché di tutte quelle contenenti fatti già oggetto, in passato, di specifiche attività di istruttoria e già archiviate, salvo che emergano nuove informazioni tali da rendere necessarie ulteriori attività di verifica;
b) *avviare un'istruttoria* per le segnalazioni che contengono elementi ragionevolmente sufficienti

per intraprendere un accertamento circa il presunto illecito segnalato.

L'obiettivo delle attività di istruttoria sulle segnalazioni è di procedere ad accertamenti circa la fondatezza dei fatti segnalati e può essere realizzata avvalendosi del supporto delle funzioni/uffici aziendali ovvero del supporto di specialisti esterni, anche in considerazione della tipologia di reato cui si riferisce la presunta violazione (es. aspetti etici correlati a comportamenti dei dipendenti, fenomeni di corruzione da parte di fornitori o partner commerciali, tematiche relative al Sistema di Gestione Sicurezza sui luoghi di Lavoro, utilizzo dei sistemi informativi aziendali, ecc.).

Sulla base degli esiti di detta istruttoria, l'O.d.V. alternativamente potrà:

a) *verbalizzare l'archiviazione* nel caso in cui la segnalazione risulti priva di riscontri, ovvero vi sia la ragionevole convinzione che non sia stata commessa una violazione;
b) *elaborare una Relazione* nei casi in cui ritenga che vi siano elementi sufficienti per valutare positivamente la fondatezza dei fatti segnalati, ovvero sia stata accertata una violazione

Nei casi in cui l'O.d.V. ritiene che le segnalazioni rivelatesi infondate siano state effettuate con dolo o colpa grave, ne informa prontamente l'organo competente (CdA, Collegio Sindacale o AD), affinché quest'ultimo possa, se del caso, adottare opportuni provvedimenti nei confronti del segnalante.

La Relazione predisposta dall'O.d.V. dovrà contenere almeno i seguenti elementi:

- la descrizione della condotta o dell'evento riscontrato;
- l'indicazione delle previsioni normative, del Modello, del Codice Etico o delle procedure aziendali che risultino essere state violate;
- i dati identificativi dell'autore della violazione, quando individuato;
- gli elementi, anche di natura documentale, comprovanti la violazione;
- una valutazione conclusiva circa la gravità degli illeciti commessi ai fini dell'applicazione delle sanzioni, fornendo adeguate indicazioni al fine di rispettare i principi di proporzionalità e di adeguatezza delle sanzioni rispetto alle violazioni.

L'Organismo invia la Relazione ai seguenti destinatari, secondo le diverse circostanze sotto indicate:

- al Consiglio di Amministrazione, nel caso in cui la violazione sia commessa da un Amministratore, da un Sindaco, dal Collegio Sindacale collegialmente considerato;
- al Collegio Sindacale, nel caso in cui la violazione sia commessa dal Consiglio di Amministrazione collegialmente considerato;
- all'AD, nel caso in cui la violazione sia commessa da un dipendente o da un terzo (consulenti, fornitori, ecc.).

I destinatari della Relazione dell'O.d.V., appena possibile e, comunque, entro trenta giorni dall'acquisizione della Relazione stessa, avvieranno il processo di contestazione della violazione come descritto nel seguente paragrafo 5.9 *"Il procedimento di irrogazione delle sanzioni"*.

In ogni caso, l'irrogazione di una delle sanzioni previste nel presente Sistema Disciplinare non precluderà alla Società il diritto di agire, anche in sede giudiziaria, nei confronti dei soggetti responsabili, per il risarcimento di tutti i danni subiti o subendi a causa della violazione commessa, ivi inclusi quelli causati dall'eventuale applicazione da parte del Giudice delle misure previste dal Decreto.

5.9. IL PROCEDIMENTO DI IRROGAZIONE DELLE SANZIONI

Il procedimento di irrogazione delle sanzioni conseguenti alla violazione del Modello si differenzia, con riguardo a ciascuna categoria di soggetti destinatari, quanto alla fase:

- della contestazione della violazione all'interessato;
- di determinazione e di successiva irrogazione della sanzione.

Il procedimento di irrogazione ha, in ogni caso, inizio a seguito della ricezione, da parte degli organi aziendali di volta in volta competenti, della Relazione con cui l'O.d.V. segnala la possibile rilevanza dell'episodio e si articola in base alla casistica di seguito illustrata:

a) Contestazione delle violazioni ed irrogazione della sanzione nei confronti di un Consigliere di Amministrazione, di un Sindaco o dell'intero CdA o dell'intero Collegio Sindacale

Il CdA informerà, con congruo anticipo rispetto alla data della riunione consiliare nella quale sarà deliberato se si è effettivamente verificata una violazione sanzionabile o meno, il soggetto interessato (Consigliere, Sindaco o Collegio Sindacale collegialmente considerato), affinché abbia conoscenza della violazione contestata, concedendogli un termine per formulare eventuali rilievi e/o deduzioni. In occasione della suddetta riunione, alla quale l'interessato sarà invitato a partecipare per essere personalmente sentito, il CdA, sulla scorta degli elementi acquisiti, adotterà le deliberazioni in merito a quanto segnalato dall'O.d.V., determinando altresì le iniziative più opportune da adottare, ed in particolare potrà comminare le sanzioni di cui ai precedenti paragrafi.

Qualora la violazione sia riferita al Consiglio di Amministrazione collegialmente considerato, il Collegio Sindacale porterà a conoscenza del CdA la violazione contestata così che possano essere formulate eventuali deduzioni. Dopo aver acquisito tutti gli elementi informativi ed ascoltato sul punto il CdA, il Collegio Sindacale determinerà le iniziative più opportune da adottare e, se del caso, procederà a convocare l'Assemblea degli Azionisti.

Resta di competenza dell'Assemblea degli Azionisti, all'uopo convocata, deliberare in merito alla revoca di uno o più componenti del Consiglio di Amministrazione o del Collegio Sindacale.

L'O.d.V. è informato delle deliberazioni assunte dal CdA ovvero dal Collegio Sindacale o dall'Assemblea degli Azionisti.

b) Contestazione delle violazioni ed irrogazione della sanzione nei confronti di un dipendente

La procedura di contestazione delle violazioni sarà espletata nel rispetto delle prescrizioni dell'art. 7 dello Statuto dei Lavoratori, nonché dei contratti collettivi applicabili e del codice disciplinare interno.

L'AD, con il supporto delle competenti Funzioni aziendali, provvederà alla contestazione dell'addebito nei confronti del dipendente mediante comunicazione scritta, informando contestualmente l'interessato della facoltà di formulare eventuali deduzioni e/o giustificazioni scritte entro cinque giorni dalla ricezione della comunicazione, nonché della facoltà di essere sentito personalmente eventualmente con l'assistenza di un rappresentante dell'associazione sindacale cui il dipendente aderisce o conferisce mandato.

Il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni

successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio. Qualora il datore di lavoro non provveda, entro dieci giorni dall'invito rivoltogli dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto. Se il datore di lavoro adisce l'autorità giudiziaria, la sanzione disciplinare resta sospesa fino alla definizione del giudizio.

L'eventuale provvedimento sanzionatorio è comunicato anche all'O.d.V., che potrà verificare la sua applicazione.

c) *Contestazione delle violazioni ed irrogazione della sanzione nei confronti di un "Terzo Destinatario"*

L'AD, con il supporto delle competenti Funzioni aziendali, previa eventuale convocazione del Terzo Destinatario ed acquisizione delle sue dichiarazioni a giustificazione della violazione addebitatagli, determinerà se detto soggetto è sanzionabile e, se del caso, stabilirà e comunicherà all'interessato la relativa sanzione, applicabile in forza della normativa vigente e dei contratti sottoscritti.

La decisione di irrogazione ovvero di non irrogazione della sanzione sarà comunicata all'O.d.V..

d) *Contestazione delle violazioni ed irrogazione della sanzione nei confronti dell'Organismo di Vigilanza*

Il CdA informa l'O.d.V. affinché abbia conoscenza della violazione contestata, concedendogli un termine per formulare eventuali rilievi e/o deduzioni. Ove l'interessato richieda di essere personalmente sentito, il CdA procede in tal senso. Di seguito il CdA, sulla scorta degli elementi acquisiti, adotta le deliberazioni in merito, determinando altresì le iniziative più opportune da adottare.

PARTE SPECIALE

1. FUNZIONE DELLA PARTE SPECIALE

La Parte Speciale del Modello ha l'obiettivo, coerentemente con i principi delineati nella Parte Generale, di definire e formalizzare per *ogni area di attività a rischio ex D.Lgs. 231/01 individuata*:

- il *potenziale profilo di rischio*, ovvero i reati che possono essere in astratto realizzati nell'area a rischio e le modalità di commissione degli stessi;
- le *attività a rischio e gli Enti coinvolti* ovvero le diverse attività aziendali a rischio e le Direzioni/Funzioni aziendali coinvolte nella loro gestione;
- i *protocolli di controllo specifici* che i Destinatari sono tenuti a rispettare, intendendosi per tali i documenti aziendali che regolamentano l'operatività della Società (per brevità "procedure"), gli specifici strumenti ed attività di controllo ritenuti rilevanti ai sensi della prevenzione dei reati di cui al D.Lgs. 231/01, applicabili alle attività ed ai processi a rischio-reato.

La presente Parte Speciale si applica ai Destinatari del Modello così come identificati nella Parte Generale dello stesso.

La Società si adopera, in linea con quanto descritto nel capitolo 4 della Parte Generale, affinché venga data ai Destinatari adeguata informativa e formazione in ordine ai contenuti della Parte Speciale.

È responsabilità dell'O.d.V. verificare l'aderenza e la concreta attuazione di quanto previsto in materia di controlli nell'ambito delle diverse aree di attività a rischio. A tal fine, le aree a rischio di cui alla presente Parte Speciale, saranno oggetto di periodiche attività di monitoraggio da parte dell'O.d.V.

I richiami alle strutture organizzative ed alle figure professionali effettuati nella presente Parte Speciale, in caso di modifiche interne dell'assetto aziendale e fino all'aggiornamento del Modello stesso, si devono intendere effettuati alle nuove strutture ovvero alle nuove figure professionali che hanno assunto i compiti e le responsabilità di quelle qui indicate.

2. PRINCIPI GENERALI DI CONTROLLO

Il sistema di controllo interno si fonda su alcuni elementi distintivi, aventi caratteristiche comuni in relazione a tutte le aree di possibile rischio di commissione dei reati nell'attività aziendale. In particolare, si illustrano di seguito i principi generali del sistema di controllo adottati dalla Società per la prevenzione di condotte illecite nello svolgimento delle attività aziendali, complessivamente considerate, e nel cui ambito si ritiene sussistere in astratto la possibilità che siano commessi i reati previsti dal Decreto.

2.1. ORGANIZZAZIONE E PROCEDURE

Teleconsys si è dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- chiara descrizione delle linee di riporto;
- conoscibilità, trasparenza e pubblicità dei poteri attribuiti (all'interno della Società e nei confronti dei terzi interessati);
- chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità.

Inoltre, detti strumenti organizzativi sono ispirati ai seguenti principi di controllo:

- separazione, all'interno di ciascun processo, tra il soggetto che assume la decisione, il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "separazione dei compiti");
- traccia scritta di ciascun passaggio rilevante del processo (c.d. "tracciabilità");
- adeguato livello di formalizzazione (procedure scritte).

In particolare:

- l'organigramma aziendale e gli ambiti e le responsabilità delle funzioni aziendali sono definiti chiaramente e precisamente mediante appositi ordini di servizio, resi disponibili a tutti i dipendenti;
- sono definite apposite policy e procedure operative che regolino la gestione ed i processi decisionali sia nelle aree "a rischio" diretto di commissione dei reati previsti dal Decreto sia nelle aree di attività ritenute strumentali alla commissione di detti reati;
- le attività di un singolo processo sono segregate per fasi e distribuite tra più funzioni e prevedono, oltre ai flussi operativi per la realizzazione delle singole attività, anche specifici momenti di controllo interno indipendente sulle stesse;
- sono previsti con chiarezza e precisione ruoli e compiti dei responsabili interni di ciascuna area a rischio, cui conferire potere di direzione, impulso e coordinamento delle funzioni sottostanti.

Nell'espletamento di tutte le operazioni attinenti alla gestione aziendale, devono, inoltre, essere rispettate le norme inerenti il sistema amministrativo, contabile, finanziario ed il controllo di gestione, nonché, in generale, la normativa applicabile.

2.2. DELEGHE E PROCURE

Le deleghe e le procure sono caratterizzate da elementi di "certezza" al fine di una chiara individuazione e delimitazione delle attribuzioni e delle responsabilità, e consentono la gestione efficiente dell'attività aziendale.

Si intende per

- "delega": un atto interno di attribuzione di funzioni e compiti;
- "procura": un atto unilaterale con cui Teleconsys attribuisce ad un singolo soggetto il potere di agire in rappresentanza della stessa.

I requisiti essenziali delle deleghe e delle procure sono i seguenti:

- i dipendenti che sottoscrivono per conto della Società impegni e rapporti contrattuali con i terzi, devono essere dotati di procura formale;
- a ciascuna procura che comporti il potere di rappresentanza nei confronti dei terzi deve corrispondere una delega interna che descriva il relativo potere di gestione;
- le deleghe devono coniugare ciascun potere alla relativa responsabilità e ad una posizione adeguata nell'organigramma aziendale;
- ciascuna delega deve definire in modo specifico ed inequivoco:
    - i poteri del delegato, precisandone i limiti;
    - il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
- al delegato devono essere riconosciuti poteri di spesa adeguati alle funzioni conferite;
- le deleghe e le procure devono essere tempestivamente aggiornate;
- qualsiasi comportamento tenuto dal procuratore/delegato in violazione dei limiti assegnatigli o di altre disposizioni di legge o aziendali, con particolare riferimento ai comportamenti che possano fondatamente coinvolgere Teleconsys nel compimento di reati previsti dal Decreto è causa di revoca immediata di tutti i poteri conferiti all'interessato.

2.3. IL CONTROLLO DI GESTIONE E LA VERIFICA DEI FLUSSI FINANZIARI

Il Controllo di Gestione è sviluppato in coerenza con le best practicies di riferimento ed articolato nelle diverse fasi di elaborazione del budget annuale e di analisi dei consuntivi periodici. Il sistema garantisce la:

- pluralità di soggetti coinvolti, in termini di congrua segregazione delle funzioni per l'elaborazione e la trasmissione delle informazioni;
- capacità di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità, attraverso un adeguato e strutturato sistema di flussi informativi e di reporting.

Parimenti, le regole per la gestione e la verifica dei flussi finanziari sono definite sulla base di principi improntati ad una sostanziale segregazione delle funzioni, tale da garantire che tutti i flussi finanziari in uscita siano richiesti, effettuati e controllati da strutture organizzative indipendenti o soggetti per quanto possibile distinti, ai quali, inoltre, non sono assegnate altre responsabilità tali da determinare

potenziali conflitti di interesse. Tale segregazione delle attività è garantita anche per quel che riguarda i flussi finanziari in entrata.

3. LE REGOLE DI CONDOTTA

3.1. PRINCIPI GENERALI

Gli Organi Sociali e tutti i dipendenti di Teleconsys sono tenuti ad osservare i seguenti principi generali:

- rigoroso rispetto di tutte le leggi ed i regolamenti che disciplinano l'attività aziendale;
- instaurazione e mantenimento di qualsiasi rapporto con terzi secondo criteri di massima correttezza e trasparenza;

È conseguentemente vietato:

- porre in essere, causare o agevolare comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle del Decreto;
- porre in essere, causare o agevolare comportamenti tali che – sebbene non costituiscano di per sé fattispecie di reato rientranti tra quelle sopra considerate – possano potenzialmente diventarlo;
- violare le regole contenute nelle procedure, nel Codice Etico, nel Modello ed in generale negli atti adottati in esecuzione dei medesimi;
- effettuare elargizioni in denaro ad esponenti della Pubblica Amministrazione ovvero di altre Società private volte ad ottenere un qualsiasi vantaggio per Teleconsys;
- distribuire omaggi e regali a soggetti terzi (esponenti della Pubblica Amministrazione ovvero soggetti privati) italiani ed esteri, o a loro familiari, al di fuori di quanto previsto dalle regole o dalle consuetudini aziendali. In particolare, è vietata qualsiasi forma di regalo, che possa influenzare l'indipendenza di giudizio del destinatario o indurlo ad assicurare un qualsiasi vantaggio a Teleconsys;
- accordare altri vantaggi di qualsiasi natura (ad es. promesse di assunzione, utilizzo di beni aziendali, ecc.) in favore di esponenti della Pubblica Amministrazione o di soggetti privati con cui Teleconsys intrattiene rapporti legati all'attività aziendale.

3.2. REGOLE DI CONDOTTA NEI CONFRONTI DI ESPONENTI DELLA PUBBLICA AMMINISTRAZIONE

Per esponenti della Pubblica Amministrazione (di seguito anche P.A.), ai fini del presente Modello, si intendono il pubblico ufficiale e l'incaricato di pubblico servizio, di cui agli artt. 357 e 358 c.p.. che, a titolo esemplificativo e non esaustivo, possiamo individuare nelle seguenti categorie:

- soggetti che svolgono una pubblica funzione legislativa o amministrativa, quali, ad esempio parlamentari e membri del Governo, consiglieri regionali, parlamentari europei e membri del Consiglio d'Europa;
- soggetti che svolgono una pubblica funzione giudiziaria, quali, ad esempio magistrati o che svolgono funzioni collegate (ufficiali e agenti di polizia giudiziaria, guardia di finanza e carabinieri, cancellieri, segretari, periti e consulenti del Pubblico Ministero tra cui i CTU del processo civile ed in genere tutti gli ausiliari del giudice, commissari liquidatori nelle procedure fallimentari, liquidatori del concordato preventivo, commissari straordinari dell'amministrazione straordinaria delle grandi imprese in crisi ecc.);

- soggetti che svolgono una pubblica funzione amministrativa, quali, ad esempio dipendenti dello Stato, di organismi internazionali ed esteri e degli enti territoriali ivi comprese le Regioni, le Province, i Comuni e le Comunità montane;
- dipendenti di altri enti pubblici, nazionali ed internazionali (ad esempio funzionari e dipendenti della Camera di Commercio, della Banca d'Italia, delle Autorità di Vigilanza, degli Istituti di Previdenza pubblica, dell'ISTAT, ecc.).

Assume particolare rilievo la circostanza che la figura del pubblico ufficiale e dell'incaricato di pubblico servizio sono individuate non sulla base del criterio della appartenenza o dipendenza da un ente pubblico, ma con riferimento alla natura dell'attività svolta in concreto dalla medesima, ovvero, rispettivamente, pubblica funzione e pubblico servizio.

Pertanto, si evidenzia che anche un soggetto estraneo alla Pubblica Amministrazione può dunque rivestire la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, quando eserciti una delle attività definite come tali dagli artt. 357 e 358 c.p. (ad es. vedasi, dipendenti di istituti bancari ai quali siano affidate mansioni rientranti nel "*pubblico servizio*", ecc.).

Gli Organi Sociali e tutti i dipendenti di Teleconsys nell'espletamento delle attività che comportino contatti con funzionari pubblici o incaricati di pubblico servizio sono tenuti ad osservare un comportamento rigoroso, conformandosi alle normative di riferimento vigenti ed alle regole di condotta definite nel Codice Etico, nel Modello e nel sistema delle procedure aziendali.

In riferimento alla gestione dei rapporti e contatti con funzionari pubblici o incaricati di pubblico servizio (ad esempio in materia fiscale, lavorativa e previdenziale, di tutela della privacy, informatica, ecc.) le procedure adottate da Teleconsys:

- prevedono specifici sistemi di controllo dei rapporti tra Teleconsys e gli organi o enti pubblici per la richiesta di informazioni, la redazione e presentazione di atti e domande, la gestione delle relative fasi istruttorie ed ispettive (ad es. mediante compilazione di schede informative, la convocazione di apposite riunioni, la verbalizzazione degli incontri);
- prevedono specifici protocolli di verifica della veridicità, completezza e correttezza di documenti da produrre e della relativa, tempestiva presentazione;
- contemplano specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- individuano, nell'ambito della funzione deputata a rappresentare Teleconsys nei confronti degli organi od enti interessati, uno o più soggetti cui conferire apposita delega e procura, e stabiliscono specifiche forme di riporto periodico dell'attività svolta sia verso l'O.d.V. che verso il responsabile della funzione competente;
- definiscono con chiarezza e precisione ruoli e compiti della funzione responsabile del controllo sulle diverse fasi di svolgimento del rapporto con i predetti organi od enti, ivi incluso l'obbligo di rendicontazione periodica all'O.d.V.;
- con particolare riferimento ai casi di accertamento ispettivo presso Teleconsys, impongono ai procuratori incaricati la redazione congiunta di un report informativo dell'attività svolta nel corso dell'ispezione, contenente, fra l'altro, i nominativi dei funzionari incontrati, i documenti richiesti e/o consegnati, i soggetti coinvolti e una sintesi delle informazioni verbali richieste e/o fornite;

- prevedono l'archiviazione e la conservazione della documentazione prodotta nonché dei modelli e verbali compilati ed inviati all'AD e all'O.d.V. in occasione delle visite ispettive.

Inoltre, nell'ambito delle regole di condotta sopra riportate, è fatto divieto di:

- porre in essere comportamenti tali da favorire qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle suddette ipotesi di reato;
- presentare dichiarazioni o fornire, in qualsiasi forma, informazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o, in generale, tali da indurre in errore ed arrecare un danno all'organismo erogatore;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli cui erano destinati;
- esercitare indebite pressioni o sollecitazioni sui pubblici agenti in vista del compimento di attività inerenti l'ufficio;
- condizionare in qualsiasi forma e con qualsiasi mezzo la libertà di determinazione di soggetti che, a qualsiasi titolo, siano chiamati a rendere dichiarazioni innanzi all'Autorità Giudiziaria;
- alterare il funzionamento di sistemi informatici e telematici o manipolare i dati in essi contenuti.

3.3. REGOLE DI CONDOTTA NEI RAPPORTI CON I TERZI

Gli Organi Sociali e tutti i dipendenti di Teleconsys nell'espletamento delle attività che comportino l'istaurazione di rapporti contrattuali di qualsiasi genere con terzi privati (acquisti, vendite, collaborazioni, intermediazioni, contratti di natura finanziaria e/o bancaria, ecc.) sono tenuti ad osservare un comportamento rigoroso, conformandosi alle normative di riferimento vigenti ed alle regole di condotta definite nel Codice Etico, nel Modello e nel sistema delle procedure aziendali ed in particolare i soggetti coinvolti nei rapporti con i terzi privati devono:

- garantire l'effettuazione di una valutazione dell'integrità, onestà ed affidabilità delle controparti contrattuali, attraverso una specifica analisi di background che consideri eticità e standing, competenze di natura tecnica, solidità patrimoniale e finanziaria delle stesse;
- effettuare attività di verifica mirate all'accertamento dell'identità delle controparti e dei soggetti per conto dei quali esse eventualmente agiscono (attraverso, ad esempio, la raccolta di dati e documentazione quali denominazione, sede legale e codice e/o domicilio fiscale, atto costitutivo e statuto, poteri di rappresentanza ed i dati identificativi degli amministratori delle controparti);
- verificare e garantire l'aggiornamento/manutenzione/diffusione delle liste interne di soggetti interessati da provvedimenti restrittivi emanati dalle preposte Autorità e Organismi nazionali (ad esempio, Unità di Informazione Finanziaria di seguito UIF, Ministero dell'Economia e delle Finanze) ed internazionali (ad esempio, OFAC, GAFI, Unione Europea).

Qualsiasi rapporto contrattuale con i terzi privati è disciplinato in modo da rendere palese che la violazione delle regole e dei principi di comportamento contenuti nel Codice Etico può determinare la risoluzione immediata del contratto e l'irrogazione di penali, salvo in ogni caso, il maggior danno.

In relazione a quanto sopra, ai Destinatari del presente Modello è fatto divieto di:

- effettuare prestazioni o elargizioni in denaro ovvero riconoscere compensi o altri vantaggi di qualsiasi tipo in favore di terzi che non trovino adeguata giustificazione nel rapporto contrattuale instaurato con gli stessi o in relazione al tipo di incarico da svolgere;
- ricevere o sollecitare elargizioni in denaro, omaggi, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, o comunque volti ad acquisire indebiti trattamenti di favore nella conduzione di qualsiasi attività aziendale, in cambio della corresponsione di denaro o benefici di ogni genere; chiunque riceva omaggi o vantaggi di altra natura non compresi nelle fattispecie consentite, è tenuto a darne comunicazione all'O.d.V. secondo le procedure stabilite.

I soggetti terzi privati, che operano per conto di Teleconsys, debbono conformarsi inoltre ai seguenti principi:

- tracciabilità e documentazione dei rapporti intrattenuti;
- gestione dei rapporti in esame esclusivamente ad opera delle funzioni aziendali competenti;
- comunicazioni dirette a tali soggetti sottoscritte nel rispetto dei poteri conferiti a soggetti aziendali;
- rispetto delle competenze aziendali e del sistema delle deleghe in essere, anche con riferimento ai limiti di spesa relativi alle funzioni ed alle modalità di gestione delle risorse finanziarie;
- corretto utilizzo delle procedure informatiche, tenendo conto delle più avanzate tecnologie acquisite in tale settore;
- segnalazione tempestiva di ogni situazione anomala alle funzioni aziendali competenti e all'O.d.V..

La Società adotta le presenti Regole di condotta anche nell'instaurazione dei rapporti di natura commerciale (acquisti o cessioni di beni o servizi) con i Soci e/o con le Società Partecipate, garantendo il rispetto delle regole del mercato e formalizzando i relativi accordi. Inoltre, detti rapporti sono gestiti nel rigoroso rispetto del principio di autonomia dei soggetti e dei principi di corretta gestione, trasparenza contabile e separatezza patrimoniale.

4. LA GESTIONE DELLE CRITICITÀ E SEGNALAZIONI ALL'ORGANISMO DI VIGILANZA

Chiunque ritenesse che eventuali attività poste in essere in Teleconsys sono, o potrebbero essere, contrarie ai principi del Modello ovvero del Codice Etico o delle procedure adottate dalla Società, è tenuto a riferire la questione all'Organismo di Vigilanza, secondo le modalità stabilite nella Parte Generale del Modello, alla quale si rinvia.

Chiunque non si attenga alla disciplina prevista nella presente Parte Speciale, ivi compreso l'obbligo di segnalazione stabilito al precedente capoverso, potrà essere soggetto a provvedimento disciplinare da parte di Teleconsys, ai sensi del Modello stesso.

L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali sancite nella presente Parte Speciale nello svolgimento dei compiti assegnati, nonché ulteriori informazioni di volta in volta ritenute utili.

I Responsabili delle Direzioni/Funzioni aziendali coinvolte nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità del processo seguito comprovante il rispetto della normativa e di quanto stabilito nel Modello, tenendo a disposizione dell'O.d.V. tutta la relativa documentazione.

5. LE AREE A RISCHIO

5.1. ATTIVITÀ COMMERCIALI E DI VENDITA DEI PRODOTTI E SERVIZI

5.1.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività commerciali e di vendita espone, in via potenziale, la Società alla commissione dei reati di:

- corruzione per l'esercizio della funzione e/o corruzione per un atto contrario ai doveri d'ufficio, e/o corruzione di persona incaricata di un pubblico servizio e pene per il corruttore, istigazione alla corruzione, induzione indebita a dare o promettere utilità, al fine di acquisire il contratto dalla PA;
- corruzione tra privati ed istigazione alla corruzione tra privati, per ottenere favori nell'ambito dello svolgimento delle attività aziendali (es.: promessa di denaro o altra utilità ad un soggetto appartenente ad una società privata, per acquisire ordini/contratti a condizioni favorevoli);
- truffa, attraverso la predisposizione di documentazione non veritiera in fase di offerta o commercializzazione dei prodotti, ad esempio attraverso l'indicazione di aspetti tecnici non veritieri o di referenze non esistenti;
- riciclaggio, qualora la Società ceda un bene, per la cui produzione è stato utilizzato denaro, beni o altre utilità provenienti da delitto non colposo;
- ricettazione nel caso in cui la Società, pur conoscendo che i prodotti ceduti siano di provenienza illecita ne garantisca la commercializzazione ottenendo condizioni particolarmente vantaggiose nella vendita;
- vendita di prodotti industriali con segni mendaci e fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale che potrebbe verificarsi se nella cessione di prodotti la Società utilizzasse segni mendaci oppure se usurpasse titoli di proprietà industriale, ovvero utilizzasse disegni, progetti, soluzioni o realizzazioni informatiche coperti da proprietà industriale; tali aspetti assumono rilevanza anche in considerazione delle vendite di prodotti con i loghi e marchi dei "Vendor";
- associazione per delinquere e associazione di tipo mafioso, terrorismo o di eversione dell'ordine democratico, nel caso in cui coloro che supportano la Società nell'attività di vendita oppure i beneficiari dei beni/servizi erogati, sono direttamente o indirettamente, legati a soggetti che intendono porre in essere tali reati;
- autoriciclaggio, se, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti non colposi di cui al D.Lgs. 231/01, le Società ottengano delle utilità che impiegano, sostituiscono o trasferiscono, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Si consideri, inoltre, che il processo di individuazione delle opportunità di vendita e di promozione commerciale per l'acquisizione di nuovi Clienti o contratti attraverso i servizi offerti da terzi agenti, intermediari o promotori commerciali, anche per singoli affari, costituisce comunque una delle modalità strumentali alla commissione dei reati sopra indicati. Inoltre, con specifico riferimento ai rischi cui si espone la Società nei rapporti con gli agenti intermediari o promotori commerciali, si rimanda anche al successivo paragrafo 4.2 *"Approvvigionamento di beni e servizi da terzi"*, potendo assimilare per tali aspetti i terzi promotori commerciali alla più generica categoria dei fornitori.

5.1.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- pianificazione e coordinamento delle strategie commerciali e di marketing, per definire gli obiettivi di vendita per area/linea di prodotto/servizio in coerenza con il mercato di riferimento;
- presidio dell'evoluzione dei prodotti/servizi per gestire l'evoluzione della domanda di mercato (es. collaborare con i "vendor" o "distributori" allo sviluppo dei prodotti/servizi per i Clienti);
- revisione ed aggiornamento obiettivi e budget in corso dell'anno;
- gestione delle quotazioni di vendita e dei prezzi;
- predisposizione e presentazione della documentazione di offerta per la partecipazione a procedure di selezione della Pubblica Amministrazione (PA) ovvero a trattative con soggetti privati;
- contatto diretto e gestione relazioni con i rappresentanti di Clienti/potenziali Clienti;
- commercializzazione prodotti con loghi e marchi dei "Vendor";
- pubblicazioni commerciali di foto ed informazioni di prodotti/servizi di terzi offerti da Teleconsys;
- utilizzo a scopi commerciali dei loghi e segni identificativi dei Clienti;
- monitoraggio del "livello vendite" sui Clienti "fidelizzati";
- negoziazione tecnica ed economica dell'Ordine/Contratto;
- formalizzazione del contratto con i Clienti rilevanti e/o conferma ed accettazione ordini dei Clienti;
- gestione degli agenti/partner commerciali;
- gestione degli eventi di marketing, qualora realizzati;
- gestione dei canali "social" della Società;

5.1.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività commerciali e di vendita dei prodotti devono essere svolte nel rispetto dei principi espressi nel Codice Etico e delle procedure della Società, nell'ambito delle quali sono definite le modalità operative, i flussi informativi, gli strumenti e le responsabilità con riferimento alla predisposizione delle offerte commerciali e della gestione delle attività commerciali tramite partner. Tali procedure prevedono, tra l'altro, quanto segue:

- con riferimento alla fase di *definizione ed approvazione delle offerte e conclusione degli accordi*:
  - le modalità operative seguite per lo svolgimento dell'attività di scouting delle opportunità e di analisi delle stesse per decidere in merito alla loro perseguibilità o meno;

- il coinvolgimento di più Direzioni/Funzioni della Società in base ai rispettivi ambiti di competenza, in un'ottica di collaborazione, vigilanza reciproca e coordinamento al fine della definizione dell'offerta tecnica e dell'offerta economica;
- i controlli idonei ad evitare il rischio di produzione di documenti incompleti o inesatti o che attestino, contrariamente al vero, l'esistenza delle condizioni o dei requisiti essenziali per partecipare alla gara e/o per l'aggiudicazione, ovvero che determinino il rischio di claims da parte di terzi o varianti in corso d'opera;
- nell'eventualità di partecipazione a gare di qualsiasi tipo indette dalla PA (italiana o estera), l'obbligo di osservare tutte le disposizioni di legge e di regolamento che disciplinano la gara, astenendosi da comportamenti che possano, comunque, turbare o influenzare indebitamente lo svolgimento della stessa;
- la gestione del processo di approvazione e sottoscrizione dell'offerta, nel rispetto dei poteri interni e delle procure conferite;
- le verifiche sulla controparte della presenza di adeguati requisiti finanziari, etici e morali, compresa l'adozione di un proprio Codice Etico da parte del Cliente ovvero, in caso negativo, la disponibilità ad accettare il Codice Etico di Teleconsys;
- l'iter di verifica ed accettazione degli ordini pervenuti dai Clienti;
- le modalità di modifica agli ordini/contratti originali (integrazioni, annullamento, ecc.);
- i contratti sottoscritti dalla Società siano, di norma, elaborati sulla base di formati standard, siano sottoposti per valutazione e condivisione alla Funzione Legale e alle Funzioni/ Direzioni interessate all'esecuzione dello stesso, al fine di recepire eventuali integrazioni/modifiche;
- la presenza di specifiche clausole contrattuali a tutela e corretto utilizzo dai diritti di proprietà intellettuale, marchi e brevetti;
- durante la fase di negoziazione dell'accordo/contratto, il soggetto che ha approvato l'offerta deve essere consultato ogni qualvolta si stiano considerando rilevanti modifiche di tipo tecnico-economico all'interno del contratto rispetto all'offerta approvata;
- l'adeguata conservazione dei contratti e di tutta la documentazione relativa alla trattativa commerciale ed alle valutazioni effettuate sul Cliente.

Con specifico riferimento alla *gestione dei canali social e degli eventuali eventi di marketing*, la Società prevede che queste attività siano svolte nel rispetto del Codice Etico, delle procedure aziendali applicabili (ad esempio procedura acquisti nel caso vengano acquisiti beni o servizi per gestire eventi o per gestire i social media) e dei seguenti protocolli:

- gli eventi di marketing non devono avere la finalità di influenzare indebitamente la decisione del potenziale Cliente ma devono essere orientati a rappresentare i prodotti e le capacità tecniche e produttive di Teleconsys;
- la gestione dei social media deve essere orientata a promuovere in maniera leale, trasparente e corretta i prodotti, i servizi e le capacità tecniche della Società e non devono essere utilizzati per denigrare un concorrente o i suoi prodotti/servizi;

- i rapporti con la stampa e con gli altri mezzi di comunicazione di massa devono svolgersi secondo gli indirizzi preventivamente fissati dal Vertice aziendale, nell'ambito dei quali assume particolare rilievo la previsione di punti di controllo sulla correttezza della notizia.

Infine, la presentazione di offerte commerciali o l'accettazione di ordini che coinvolgano soggetti stranieri residenti in Paesi c.d. "paradisi fiscali" o a rischio terroristico, deve essere integrata da un'attenta valutazione del "rischio Paese" avuto riguardo al sistema di governo ed amministrazione, al Cliente specifico con il quale si prevede di intrattenere i rapporti, alla normativa vigente ed alle prassi generalmente in uso in detta area geografica, al regime fiscale e di trasparenza delle informazioni finanziarie del Paese di residenza; i risultati di detta valutazione sono formalizzati, sottoscritti e conservai agli atti della Società.

5.2. GESTIONE DEGLI ACQUISTI DI BENI E SERVIZI DA TERZI

5.2.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività di acquisto dei beni e servizi espone, in via potenziale, la Società alla commissione dei reati di:

- ricettazione, nell'ipotesi di acquisto di beni provenienti da un qualsiasi delitto ovvero nel caso di acquisto di beni di utilità aziendale corrispondendo alla controparte un pagamento evidentemente inferiore rispetto a quello richiesto dai parametri di mercato, con la consapevolezza che, anche per il basso costo dei beni acquistati, essi sono di provenienza illecita (ad esempio provengono da un furto);
- corruzione ed istigazione alla corruzione tra privati nell'ipotesi in cui ad esempio un referente della Società dia o offra/prometta denaro o altra utilità al fornitore per ottenere un indebito beneficio/utilità non dovuto quale uno sconto fuori mercato o anticipazione delle consegne;
- riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita. Tale reato potrebbe configurarsi in astratto ad esempio nel caso in cui la Società si accordi con il fornitore per eludere le regole in tema di tracciabilità dei flussi finanziari;
- autoriciclaggio, nel caso in cui, a seguito della commissione o del concorso in commissione di un delitto non colposo tra quelli previsti nell'area a rischio in oggetto, si ottengano delle utilità che sono impiegate in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa;
- i delitti contro la personalità individuale, i reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, i reati ambientali nonché il reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare. Tali reati potrebbero in astratto essere realizzati in concorso con i fornitori/appaltatori per attività da questi svolta comunque sotto il controllo di Teleconsys, consentendo dei risparmi economici anche nell'acquisto.

Inoltre, il processo di approvvigionamento potrebbe in via astratta essere lo strumento attraverso il quale viene realizzata la corruzione (ad esempio con l'assegnazione di incarichi a persone o società vicine o gradite ai soggetti pubblici, per ottenere favori nell'ambito delle attività della Società). L'indebito beneficio, ottenuto per il tramite del fornitore esterno, è l'elemento costitutivo del reato in oggetto, da associare alla qualità di pubblico ufficiale o incaricato di pubblico servizio del soggetto passivo ed all'atto d'ufficio da compiere, omettere o ritardare.
Infine, non si può escludere il rischio di commissione dei seguenti reati:

- delitti con finalità di terrorismo o di eversione dell'ordine democratico, nel caso in cui si forniscano, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendono porre in essere reati di terrorismo, attraverso la selezione e/o gestione di fornitori / subappaltatori, ottenendone un vantaggio economico (ad esempio condizioni economiche fuori mercato);
- delitti di associazione per delinquere e associazione di tipo mafioso e scambio elettorale politico – mafioso, nel caso in cui, a titolo esemplificativo, si stabilisca un patto associativo tra rappresentanti delle Società e fornitori, per:
    - alterare i risultati delle gare al fine di spartire i benefici economici derivanti da tale comportamento, attraverso, a titolo esemplificativo la costituzione a favore delle Società di fondi extra contabili utilizzabili per fini corruttivi o l'ottenimento di un significativo risparmio economico sulle forniture;

- attribuire degli appalti a ditte indicate da esponenti dell'associazione di tipo mafioso per evitare danneggiamenti dell'operatività aziendale.

5.2.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalla Società come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- definizione di strategie di acquisto in linea con le esigenze commerciali e di "commessa/progetto";
- individuazione esigenze e/o definizione del "piano di committenza" delle commesse;
- definizione dei fabbisogni puntuali di acquisto di beni e servizi non destinati alle commesse/progetti;
- revisione ed aggiornamento obiettivi e budget in corso dell'anno;
- qualifica dei fornitori e valutazione della loro affidabilità;
- gestione della qualifica/certificazioni dei beni acquistati (ove richiesto);
- analisi comparata delle quotazioni e procedure di selezione del fornitore;
- negoziazione dei prezzi e definizione degli accordi contrattuali;
- emissione dell'Ordine di Acquisto o del contratto e dei connessi adempimenti;
- ricezione del bene/servizio, monitoraggio dell'attività svolta dai fornitori e collaudi;
- certificazione che il bene/servizio sia stato fornito/svolto in linea con quanto richiesto;
- gestione di eventuali problemi e contestazioni con i fornitori

5.2.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La Società, oltre a quanto già indicato nel Codice Etico, prevede l'obbligo per chi si occupa della selezione di fornitori e consulenti (di seguito per brevità "fornitori") di verificare l'eticità e la solidità patrimoniale e finanziaria della controparte contrattuale, sulla base di alcuni indicatori/documenti rilevanti.

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto di quanto sopra, delle procedure aziendali e dei seguenti principi di riferimento:

- la definizione delle principali attività nonché dei ruoli e delle responsabilità nel processo di acquisizione di beni e servizi, garantendo in ogni fase un'adeguata separazione dei compiti. Più in particolare si riportano di seguito gli elementi cardine:
  - per quel che riguarda la fase di *richiesta di acquisto*, questa deve garantire un'adeguata formalizzazione. Le richieste di acquisto devono essere autorizzate secondo uno specifico iter, e devono rientrare nell'ambito del budget approvato;
  - in fase di *selezione e scelta delle offerte di fornitura*, deve essere garantito/a:
    - un adeguato flusso informativo tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;

  - il ricorso a criteri di valutazione oggettivi, trasparenti e documentabili, in conformità ai principi del Codice Etico e l'evidenza delle motivazioni in merito alla scelta dei fornitori;
  - la verifica in via preventiva delle informazioni disponibili (incluse informazioni finanziarie) sui fornitori, per accertare la loro rispettabilità e la legittimità della loro attività, prima di instaurare con questi rapporti d'affari. Qualora ritenuto necessario si procede alla richiesta di alcuni documenti e/o alla verifica dei dati pregiudizievoli pubblici;
  - almeno per le offerte di importi rilevanti e quando le condizioni di mercato lo permettono la richiesta di una pluralità di preventivi; gli acquisti "vincolati" ad un unico fornitore sono adeguatamente motivati in forma scritta;
- in fase di *definizione dell'ordine/contratto e sua sottoscrizione* devono essere previste le seguenti attività:
  - definizione di condizioni economiche e tecniche coerenti con la tipologia di fornitura richiesta;
  - inserimento di clausole standard, definite con il supporto della Funzione Legale, che impongano oltre al rispetto della legge (con particolare riferimento al rispetto della legge sulla tutela del segreto industriale, del lavoro, della salute e sicurezza sul lavoro e dell'ambiente), specifiche tutele per la Società a fronte del rischio di commissione dei reati di cui al D.Lgs. 231/01, a garanzia della qualità della merce consegnata e della provenienza (i fornitori devono assicurare che la provenienza reale della merce corrisponda a quella dichiarata) i diritti di proprietà intellettuale e le regole di trasparenza nei flussi di pagamenti;
  - sottoscrizione dell'ordine/contratto di fornitura da parte di soggetto della Società dotato di idonea procura in tal senso;
- la fase di *ricezione, controllo e valutazione della fornitura e di autorizzazione al pagamento* deve prevedere che:
  - per quanto possibile, la ricezione/controllo dei beni/servizi sia effettuato da soggetto (richiedente della fornitura) diverso da chi contabilizza la fattura del fornitore e da chi effettua il pagamento della fornitura/prestazione;
  - eventuali criticità o difficoltà di qualsiasi genere nell'esecuzione dei rapporti contrattuali, ivi inclusi eventuali inadempimenti o adempimenti parziali di obbligazioni contrattuali, siano evidenziati in forma scritta e gestiti dalle Direzioni/Funzioni aziendali competenti in conformità agli accordi contrattuali, nonché nel rispetto della legge;
  - l'attività prestata dal fornitore sia debitamente documentata e la Direzione/Funzione che si è avvalsa della sua opera, attesti l'effettività della prestazione, prima della liquidazione dei relativi compensi;

- l'archiviazione in formato cartaceo/informatico dei dati/documenti/atti predisposti nel corso delle attività (richieste di offerta, motivazione della scelta, analisi di benchmarking, ecc.), per assicurare la tracciabilità del processo di gestione degli acquisti di beni e servizi;

- che il fornitore deve prendere visione del Codice Etico della Società e sottoscrivere una dichiarazione di accettazione dello stesso (o in alternativa dichiarare di avere adottato un proprio Codice Etico con principi analoghi a quelli presenti nel Codice Etico di Teleconsys) e che in caso di violazione delle norme previste dallo stesso, la possibilità da parte della Società di comminare adeguate sanzioni contrattuali.

Infine, con specifico riferimento agli *incarichi di consulenza o prestazione professionale assegnati alle persone fisiche*, oltre a quanto precedentemente disciplinato, ove applicabile, Teleconsys assicura anche:

- limitazioni di cumulabilità nel conferimento degli incarichi allo stesso consulente nel medesimo periodo;
- l'omogeneità di forma e contenuto dei contratti mediante l'adozione di un modello uniforme, salve le eventuali peculiarità del caso concreto;
- l'individuazione dei rappresentanti della Società delegati a negoziare, stipulare e controllare detti contratti, nonché dei soggetti incaricati di verificarne la compatibilità con le regole aziendali;
- la legittimità delle clausole contrattuali e la loro idoneità a tutelare l'interesse sociale;
- il possesso da parte del consulente di requisiti soggettivi di affidabilità e competenze professionali necessari per lo svolgimento dell'incarico;
- una costante attività di supervisione e monitoraggio delle attività svolte dal professionista per tutta la durata del contratto, in modo, tra l'altro, da garantirne la rispondenza alle effettive esigenze aziendali ed il perseguimento degli obiettivi proposti;
- ove non siano previste altre forme di evidenze documentali circa le prestazioni professionali effettuate, la redazione da parte del professionista di un rapporto sull'attività svolta a conclusione dell'incarico.

5.3. REALIZZAZIONE COMMESSE, "DELIVERY" E SERVIZI

5.3.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Il processo di gestione della commessa e di delivery verso i Clienti finali espone le Società alla commissione (o di concorso alla commissione) dei reati:

- di vendita di prodotti industriali con segni mendaci e di fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale, nell'ipotesi in cui nello svolgimento delle attività produttive si commettano i reati in questione;
- di ricettazione, nell'ipotesi di utilizzo, nelle diverse fasi produttive, di risorse di provenienza illecita;
- di corruzione tra privati ed istigazione alla corruzione tra privati nell'ipotesi in cui un referente delle Società corrompa o tenti di corrompere, anche per interposta persona, ad esempio un fornitore o un Cliente al fine di ottenere durante le fasi di produzione un indebito beneficio/utilità non dovuto o per evitare che siano evidenziate delle problematiche riscontrate nello svolgimento delle attività di produzione (difetti, malfunzionamenti, o non conformità dei prodotti consegnati);
- corruzione, istigazione alla corruzione, induzione indebita a dare o promettere utilità, nei casi di una gestione poco trasparente nelle varie fasi di indirizzo e controllo della fornitura versa la PA ad esempio, in cambio di utilità, si possono indurre i rappresentati della PA ad accettare forniture non conformi, ad omette di comminare le penali ovvero si congruiscono ed approvano varianti tecniche ed economiche non giustificate dalle effettive esigenze;
- di truffa e truffa aggravata per il conseguimento di erogazioni pubbliche si potrebbero configurare qualora, nell'ambito della verifica del rispetto delle scadenze e delle criticità, da parte della PA committente, i soggetti coinvolti si adoperino per mascherare, nascondere e/o non comunicare eventuali criticità di natura tecnica che non consentirebbero l'approvazione del SAL, al fine di alterare i reali costi della commessa ed indurre in errore la PA nell'erogazione dei contributi pubblici sulla scorta della condotta fraudolenta;
- di autoriciclaggio nell'ipotesi di impiego di beni tramite l'utilizzo di utilità provenienti dalla commissione (anche in concorso) di delitti non colposi;
- reati contro la personalità individuale e di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, nell'ipotesi in cui tali condotte siano astrattamente commesse nell'ambito di attività produttive all'interno di aree aziendali e/o comunque sotto il controllo delle Società.

Infine, con riferimento ai reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro e sulla tutela dell'ambiente si rinvia alle analisi contenute nel paragrafo 5.7 *"Gestione della Salute e Sicurezza nei luoghi di lavoro e dell'Ambiente*".

5.3.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate come a potenziale rischio nella presente area a rischio, sebbene differenti e specifiche in ogni Società, possono essere riepilogate come segue:

- pianificare la commessa (aspetti tecnici, economici e tempistiche) e verificarne l'avanzamento;
- definire gli standard produttivi o gli SLA per servizi ICT;
- verifiche e adempimenti amministrativi propedeutici all'avvio delle attività (contratti, garanzie, autorizzazioni, ecc.);
- attività di indirizzo dei fornitori durante l'esecuzione del contratto;

- verifica formale degli avanzamenti periodici in occasione dei SAL;
- gestione delle eventuali criticità di natura tecnica;
- monitoraggio e rispetto SLA per servizi ICT;
- attivazione delle licenze;
- verifiche di conformità e collaudi;
- autorizzazione all'emissione delle fatture da parte del Committente;
- verifica presupposti ed autorizzazione atti modificativi ed integrativi dei contratti (proroghe, varianti, ecc.);
- gestione contestazioni (sia nei confronti dei fornitori sia nei confronti dei clienti);
- effettuare il "controllo qualità";
- garantire il rispetto delle norme in materia di sicurezza nei luoghi di lavoro e di ambiente;
- programmare le spedizioni e consegnare il prodotto, coordinando i flussi logistici.

5.3.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La Società, ai fini dell'attuazione delle regole e dei divieti relativi allo svolgimento delle attività di gestione delle commesse, comprendente a titolo esemplificativo e non esaustivo, anche le fasi di progettazione e realizzazione dei sistemi, la rendicontazione delle attività svolte, il controllo di qualità e del rispetto dei requisiti tecnici, la consegna ed il collaudo nonché gli eventuali ulteriori servizi di assistenza al cliente, adotta le seguenti regole di condotta:

- il personale coinvolto nelle attività di realizzazione dei sistemi/prodotti/servizi deve attenersi a quanto disciplinato all'interno dei Manuali aziendali, ivi comprese le procedure e le istruzioni operative vigenti in Teleconsys;
- nell'esercizio dei rapporti contrattuali, devono essere esclusivamente consegnati ovvero utilizzati beni dichiarati o pattuiti con i clienti (per origine, provenienza, qualità o quantità).

In relazione a quanto sopra, le procedure adottate prevedono:

- apposite verifiche per accertarsi che un prodotto sviluppato internamente non sia già stato oggetto di brevetto da parte di terzi;
- apposite clausole contrattuali nei confronti di fornitori e clienti, che possono prevedere restrizioni circa l'utilizzo di marchi/brevetti, al fine di tutelare la titolarità dei diritti di proprietà industriale;
- che, in caso di collaborazioni con partner, le parti interessate concordino esplicitamente i diritti di proprietà industriale negli accordi di collaborazione;
- che la tutela dei diritti di proprietà industriale ed il coordinamento nella gestione di tutti i brevetti e marchi registrati sia svolta durante la gestione di ogni commessa/incarico.

Relativamente all'attività in capo alla *struttura organizzativa che coordina le attività operative di realizzazione dell'incarico*, la Società assicura le seguenti attività di monitoraggio:

- la struttura ha il compito di gestire e controllare tutte le attività di commessa secondo le regole aziendali e nel pieno rispetto delle policy, procedure o manuali operativi in essere;
- al fine di documentare formalmente la conclusione del Progetto, la consegna dei prodotti (o altri "*deliverables*") viene sottoposta a controlli di conformità e viene formalmente registrata con

adeguate evidenze documentali ovvero collaudi; nel caso di fornitura di servizi viene eventualmente rilasciato al Cliente un attestato di prestazione eseguita ("Attestazione Fine Progetto");

- tutte le attività relative alla realizzazione di prodotti ed esecuzione di servizi vengono svolte nel rispetto delle regole aziendali per la tutela dei diritti di proprietà industriale (Intellectual Property Rights - IPR), in particolare, possono essere utilizzati componenti/prodotti brevettati da terzi solo previa autorizzazione formale nell'ambito del contratto;
- in caso di appalto a terzi di parte del processo produttivo, è necessario verificare che chi esegue il lavoro abbia le necessarie autorizzazioni ai sensi della legge e sia mantenuta evidenza di tutta la documentazione che attesti la tracciabilità del prodotto;

Con specifico riferimento *all'attività di Project Management*, la Società prevede i seguenti presidi organizzativi e di controllo:

- costituzione di un gruppo di lavoro (Team di Commessa), ove necessario anche interfunzionale, responsabile dello sviluppo e della gestione del progetto fino alla conclusione dell'intero ciclo di vita;
- individuazione di un responsabile del Team (o anche Project Manager di commessa) che ha il compito di:
  - coordinare tutte le attività previste per la gestione tecnica ed amministrativa della commessa e relazionare sull'andamento, segnalando eventuali criticità sia tecniche sia relazionali con i clienti, i fornitori ed i partner in RTI (ove presenti);
  - verificare la corretta rendicontazione dell'impegno da parte delle risorse interne;
  - monitorare i contratti di fornitura di beni e servizi riferibili alla commessa, verificando le relative prestazioni;
  - gestire i rapporti con i partner in RTI (ove presenti), monitorando anche tutti gli aspetti relativi all'utilizzo condiviso di opere dell'ingegno e segni distintivi;
  - assicurare la predisposizione ed accurata archiviazione, anche dopo la conclusione delle attività di commessa, di tutta la documentazione rilevante afferente al contratto.
- supervisione del Project Manager di commessa al fine di monitorare il corretto adempimento dell'incarico assegnato;
- un adeguato flusso informativo tra il Project Manager e le altre funzioni aziendali coinvolte (es. Purchasing, Legal, CFO, ecc.) in un'ottica di collaborazione, vigilanza reciproca e coordinamento;

In relazione agli aspetti relativi alla tutela della sicurezza sul lavoro e dell'ambiente si rinvia agli specifici paragrafi della presente Parte Speciale del Modello

5.4. SELEZIONE, GESTIONE, FORMAZIONI ED AMMINISTRAZIONE DEL PERSONALE

5.4.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le attività di selezione, gestione e amministrazione del personale, sia svolte direttamente sia svolte nell'ambito del contratto di servizio con professionisti esterni, espongono, in via potenziale, la Società alla commissione (o al concorso nella commissione) dei seguenti principali reati:

- impiego di cittadini di paesi terzi il cui soggiorno è irregolare, nel caso in cui la Società impieghi personale straniero sprovvisto di regolare permesso di soggiorno ovvero in caso di mancato monitoraggio in merito alla validità del permesso di soggiorno presentato inizialmente dalla risorsa assunta;
- malversazione a danno dello Stato o di altro ente pubblico, indebita percezione di erogazioni a danno dello Stato e truffa aggravata per il conseguimento di erogazioni pubbliche, nelle fasi di progettazione dei piani formativi annuali e pluriennali con l'attivazione dei processi di formazione finanziata e correlata rendicontazione;
- corruzione, corruzione tra privati ed istigazione alla corruzione tra privati. Al riguardo, occorre considerare che il processo di assunzione del personale e di progressione di carriera costituisce una delle modalità strumentali per ottenere favori nell'ambito dello svolgimento delle attività della Società, ad esempio attraverso l'assunzione o il riconoscimento di promozioni/avanzamenti di carriera/aumenti di stipendio/altre utilità di persona "vicina" o "gradita" a soggetti pubblici o assimilabili o a soggetti privati. Inoltre, la fase di definizione delle politiche di incentivazione potrebbe costituire un potenziale supporto alla commissione dei reati citati, attraverso il riconoscimento di bonus "falsati/gonfiati" per rendere disponibili somme di denaro utilizzabili per fini corruttivi.

Infine, non si può escludere che potrebbero inoltre configurarsi in via astratta:

- il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, ad esempio attraverso l'assunzione di persona "vicina" a chi è tenuta a rendere dichiarazioni all'autorità giudiziaria ovvero l'attribuzione di un bonus "gonfiato" o la promozione di una persona gradita a chi deve rilasciare dichiarazioni all'autorità giudiziaria;
- i delitti con finalità di terrorismo o di eversione dell'ordine democratico, nel caso in cui si forniscano, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendono porre in essere tali reati.

5.4.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalla Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- formalizzazione fabbisogni e definizione dei requisiti professionali richiesti;
- individuazione, valutazione e selezione dei candidati per l'assunzione del personale e conseguenti trattative;
- sottoscrizione del contratto di assunzione;
- gestione amministrativa del personale (presenze, straordinari, ferie, permessi, ecc.);
- rapporto con il consulente del lavoro che si occupa dell'elaborazione delle buste paga;
- autorizzazione, gestione e rimborsi spese delle trasferte;

- sistema di incentivazione e premialità (benefit, interventi retributivi, progressioni di carriera, ecc.);
- percorsi di formazione e delle qualifiche/certificazioni professionali.

5.4.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto di quanto indicato nel Codice Etico, nonché dalle procedure aziendali che prevedono almeno quanto segue:

- per quanto riguarda il processo di *selezione e assunzione di personale*:
  - le richieste di nuovo personale devono trovare adeguata previsione e copertura nel budget relativo al fabbisogno di organico approvato dal Vertice Aziendale;
  - nella fase di individuazione del candidato da assumere, per evitare un'eccessiva concentrazione del potere decisionale in capo ad una persona, deve essere previsto il coinvolgimento di una pluralità di soggetti, ai quali sono chiaramente attribuiti ruoli distinti (propositivi, autorizzativi, di coordinamento e di controllo del rispetto della procedura di selezione). Inoltre, in tale fase deve essere garantito/a:
    - la tracciabilità delle fonti dei curricula in fase di acquisizione e di gestione degli stessi (inserzioni, domande spontanee, presentazioni interne, ecc.);
    - l'individuazione di una rosa di candidati (salvo casi in cui si presenti un solo candidato per le posizioni aperte);
    - la formalizzazione delle varie fasi del processo di scelta della risorsa, mediante la compilazione di un form in cui riportare i principali aspetti del colloquio svolto ed il relativo giudizio, a garanzia della tracciabilità delle scelte effettuate;
  - in fase di formulazione dell'offerta di assunzione, devono essere previste le seguenti attività:
    - verificare l'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti;
    - garantire che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti a lui assegnati;
    - prevedere che il contratto di assunzione sia sempre sottoscritto da persona dotata di idonea procura in tal senso;
    - verificare, in caso di assunzione di personale extracomunitario, la regolarità del permesso di soggiorno;
    - definire un kit di documenti da richiedere al candidato prima della sua assunzione al fine di verificare l'esistenza di adeguati requisiti etici e morali;
  - in fase di assunzione, devono essere previste le seguenti attività:
    - ottenimento della firma del neoassunto di impegno al rispetto del Codice Etico e del Modello della Società;
    - informativa al neoassunto relativamente a:

- caratteristiche della funzione e delle mansioni da svolgere;
- elementi normativi e retributivi, come regolati dal Contratto Collettivo Nazionale di Lavoro e da eventuali contratti aziendali;
- norme e procedure da adottare per evitare i possibili rischi per la salute e la sicurezza associati all'attività lavorativa;
- regole generali e norme di comportamento alle quali tutti i dipendenti devono attenersi quali ad esempio Modello ex D.Lgs. 231/01, Codice Etico, "social media policy", disposizioni in materia di *"Privacy"*, ecc.;

  - esecuzione degli obblighi nei confronti degli enti pubblici di riferimento;

- l'archiviazione in formato cartaceo/informatico dei dati/documenti/atti predisposti nel corso delle attività (curricula, esito del colloquio, valutazioni, lettere di assunzione, ecc.), per assicurare la tracciabilità del processo di selezione ed assunzione;

- per quanto riguarda il *processo di gestione del personale*:
  - la definizione delle principali attività nonché dei ruoli e delle responsabilità nel processo di gestione e sviluppo del personale;
  - la gestione degli eventuali piani di incentivazione del personale con particolare riferimento alla definizione di: (i) livelli professionali di applicazione; (ii) numero e tipologia di obiettivi da assegnare; (iii) modalità di calcolo della componente variabile della retribuzione;
  - definizione formale degli obiettivi basata su criteri di specificità, oggettività, misurabilità, nonché realizzabilità;
  - formalizzazione e approvazione dell'esito delle valutazioni delle performance del personale ispirata a principi di correttezza e trasparenza e che l'erogazione degli incentivi e bonus sia basata sul collegamento diretto con gli obiettivi raggiunti;
  - l'archiviazione in formato cartaceo/informatico dei dati/documenti/atti predisposti nel corso delle attività, per assicurare la tracciabilità del processo di progressioni di carriera, assegnazione di bonus, ecc.;

- per quanto riguarda il processo di *amministrazione* del personale:
  - i rapporti con i fornitori di servizi professionali per le elaborazioni delle partite stipendiali devono essere formalizzati e prevedere in maniera chiara i rispettivi ambiti di competenza e adeguate regole di "tracciabilità" dei rispettivi flussi informativi oltre che il rigoroso rispetto delle norme del Codice Etico di Teleconsys.
  - le regole per la rilevazione delle presenze e la verifica delle stesse;
  - le richieste e il rilascio delle autorizzazioni per ferie e permessi e le modalità di comunicazioni di malattie e tutto ciò che concerne la determinazione del costo del personale;
  - l'autorizzazione alle trasferte e le regole per i rimborsi spese ai dipendenti;

- laddove necessario, la definizione di uno scadenziario circa il mantenimento della regolarità del permesso di soggiorno nel tempo per il personale extracomunitario assunto a tempo indeterminato/determinato;
- l'assegnazione di eventuali strumenti di lavoro (ad esempio autovetture, sim, telefoni, tablet), mediante l'utilizzo di apposite/i comunicazioni/moduli standard sottoscritti per accettazione, e contenenti anche il riferimento al rispetto del Modello, del Codice Etico e, più in generale, delle disposizioni della Società e della legislazione vigente;
- il rispetto di tutte le disposizioni normative in materia di lavoro e di tutela della Privacy;

5.5. AMMINISTRAZIONE, FINANZA, CONTROLLO ED OPERAZIONI SUL CAPITALE

5.5.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le attività della presente area a rischio, sia svolte direttamente sia svolte nell'ambito del contratto di servizio per prestazioni professionali, espongono, in via potenziale, la Società ai rischi di commissione dei seguenti principali reati:

- false comunicazioni sociali;
- fatti di lieve entità (riferito alle false comunicazioni sociali);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

Tali reati potrebbero configurarsi in via astratta attraverso una non corretta gestione delle attività relative all'area in analisi che hanno impatto sulla rappresentazione della situazione patrimoniale, economica e finanziaria delle Società, ad esempio, attraverso la contabilizzazione di poste transazionali fittizie e/o errate in tutto o in parte, l'omessa contabilizzazione di poste transazionali, la modifica/alterazione dei dati contabili presenti sul sistema informatico, l'esposizione di fatti materiali rilevanti non corrispondenti al vero, sopravvalutazione o sottovalutazione delle poste estimative/valutative di bilancio, l'omissione di informazioni la cui comunicazione è imposta dalla legge, circa la situazione economica, patrimoniale o finanziaria della Società.

Inoltre, le attività connesse alle operazioni sul capitale (quali ad esempio l'acquisto o la sottoscrizione, fuori dei casi consentiti dalla legge, di azioni o quote sociali, la riduzione del capitale o la fusione con altra società o una scissione in violazione degli articoli 2306, 2445 e 2503 c.c.) possono, in via potenziale, ledere l'integrità del capitale sociale e le ragioni dei creditori e, quindi, esporre le Società al rischio di commissione del reato di illecite operazioni sulle azioni e del reato di operazioni in pregiudizio dei creditori.

Per completezza di analisi, le attività in esame possono essere considerate strumentali per la commissione dei reati di:

- corruzione ed istigazione alla corruzione, sia verso la PA sia tra privati. In particolare, una gestione poco trasparente e scorretta delle registrazioni contabili e dei flussi monetari e finanziari potrebbe portare alla costituzione di "disponibilità" strumentali alla realizzazione di tali reati, ad esempio, attraverso:
  - la contabilizzazione di poste fittizie (es. la contabilizzazione di fatture false di fornitori per prestazioni inesistenti);
  - l'omessa contabilizzazione di poste per la costituzione di fondi utilizzabili per fini corruttivi;
  - l'utilizzo dei conti correnti della Società per rendere disponibili somme di denaro a fini corruttivi;
  - il pagamento di fatture fittizie/false (in tutto o in parte) per creare delle "disponibilità";
  - il riconoscimento di rimborsi spese o anticipi fittizi in tutto o in parte per ottenere "disponibilità";
- truffa ai danni dello Stato o di altro ente pubblico. Tale reato potrebbe astrattamente configurarsi nel caso in cui vengano falsificati, con l'obiettivo di ottenere un profitto i dati delle dichiarazioni fiscali/contributive;

- ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita. Tali reati potrebbero astrattamente configurarsi attraverso la gestione dei flussi finanziari connessi con le attività di gestione:
  - degli incassi derivanti dai contratti attivi e dalle vendite;
  - dei pagamenti a fronte degli acquisti.
- autoriciclaggio nel caso in cui, a seguito della commissione o del concorso in commissione di un delitto non colposo tra quelli previsti nell'area a rischio in oggetto, la Società ottenga delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Infine, in via astratta, non si possono escludere i rischi riferibili alle seguenti possibili condotte illecite:

- delitti con finalità di terrorismo o di eversione dell'ordine democratico, nel caso in cui si forniscano, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendono porre in essere reati di terrorismo;
- delitti di associazione per delinquere e associazione di tipo mafioso e scambio elettorale politico – mafioso, nel caso in cui, la Società procacci risorse finanziarie da destinare a soggetti a loro riconducibili.

Per ulteriori possibili reati "societari" si rinvia alle analisi del rischio contenute nel successivo paragrafo 2.11 *"Affari societari e rapporti con Società di Revisione, Collegio Sindacale e Soci".*

5.5.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- predisposizione del piano e del budget annuale;
- analisi periodica degli scostamenti rispetto al budget;
- ricezione, verifica e registrazione delle fatture dei fornitori;
- emissione delle fatture attive;
- effettuazione delle scritture contabili per rilevare i fatti aziendali in corso d'anno;
- effettuazione delle valutazioni e correlate scritture contabili di assestamento/rettifica per la predisposizione del bilancio;
- gestione della fiscalità diretta ed indiretta;
- predisposizione del progetto di bilancio da sottoporre all'approvazione del CdA e, quindi, dell'Assemblea dei Soci;
- gestione dell'inventario dei beni di proprietà della Società;
- operazioni sul capitale sociale/patrimonio netto;
- gestione dei pagamenti;
- gestione degli incassi;
- gestione mutui e finanziamenti a medio/lungo;

- gestione dei rapporti con gli istituti di credito;
- gestione delle garanzie attive e passive;
- gestione delle piccole casse;
- gestione delle polizze assicurative.

5.5.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La Società, in riferimento all'attività di gestione di tenuta della contabilità, predisposizione del bilancio e di gestione della fiscalità, della tesoreria e della finanza aziendale, adotta le seguenti **regole di condotta:**

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire agli azionisti ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, a beneficio dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento degli Organi Sociali, agevolando ogni controllo di gestione previsto per legge, nonché la libera e corretta formazione della volontà assembleare;
- evitare di porre in essere operazioni simulate o di diffondere notizie false su Teleconsys o sulle sue società partecipate;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste nei confronti di autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate;
- tutti i rapporti di natura finanziaria di investimento e disinvestimento sono normalmente tenuti con soggetti di cui alla Direttiva 2005/60/CE (II Direttiva antiriciclaggio), gli Intermediari Finanziari, tra cui a titolo esemplificativo e non esaustivo:
  - banche, istituti di moneta elettronica, Sim, Sgr, Sicav;
  - enti creditizi o finanziari comunitari;
  - enti creditizi o finanziari situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalla Direttiva;
  - amministrazione pubblica di Paese comunitario;
- tutte le operazioni di natura commerciale, finanziaria e societaria derivanti da rapporti continuativi ed occasionali con Soggetti Terzi (ad esclusione degli Intermediari Finanziari) devono essere precedute da un'adeguata attività di verifica volta ad accertare l'assenza del rischio di coinvolgimento nella commissione dei reati di riciclaggio, ricettazione ed impiego di denaro, beni o utilità di provenienza illecita, attraverso una chiara identificazione di:
  - controparte;
  - scopo, natura e struttura legale-fiscale dell'operazione;
  - valore complessivo ed unitario degli strumenti utilizzati nell'operazione;

- tutti gli incassi e i pagamenti derivanti da rapporti di acquisto o vendita di partecipazioni, altri rapporti intercompany, aumenti di capitale, incasso dividendi, ecc. sono regolati esclusivamente attraverso il canale bancario, l'unico atto ad assicurare, grazie ai moderni sistemi elettronici e telematici, adeguati livelli di sicurezza, tracciabilità ed efficienza nelle operazioni di trasferimento di denaro tra operatori economici;
- tutta la documentazione relativa alle operazioni sopra indicate deve essere archiviata e conservata dalle funzioni aziendali competenti;
- tutte le operazioni sui conferimenti, sugli utili e sulle riserve, le operazioni sul capitale sociale, nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle norme di legge applicabili, delle regole di corporate governance di valutazione ed analisi delle suddette operazioni, che rendano possibile tracciare tutte le attività svolte (ad es. stime, perizie) e, da parte dei responsabili delle funzioni coinvolte, controllarne ogni singola fase.

Nell'ambito dei suddetti comportamenti, è richiesto di operare secondo i principi di massima correttezza e trasparenza e, in particolare, a titolo semplificativo*:*

- restituire conferimenti all'azionista o liberarlo dall'obbligo di eseguirli, solo nei casi di legittima riduzione del capitale sociale;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati completi, accurati, veritieri e rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria;
- comunicare in maniera completa i dati e le informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria;
- ripartire utili o acconti su utili effettivamente conseguiti e non destinati per legge a riserva;
- acquistare o sottoscrivere azioni proprie o di società partecipate solo nei casi previsti dalla legge, assicurando così l'integrità del capitale sociale;
- effettuare riduzioni del capitale, fusioni o scissioni, nel rigoroso rispetto delle disposizioni di legge a tutela dei creditori;
- collaborare lealmente all'esercizio delle funzioni di controllo dell'azionista, del collegio sindacale o della società di revisione ovvero alle attività di vigilanza anche in sede di ispezione da parte delle autorità competenti;
- effettuare trasferimenti di denaro contante o di libretti di deposito bancari o postali solo con modalità che assicurino la tracciabilità dell'operazione e dei soggetti coinvolti nelle transazioni (es. tramite banche, istituti di moneta elettronica o Poste Italiane S.p.A.);
- effettuare richieste di rilascio ed utilizzo di moduli di assegni bancari e postali solo con clausola di non trasferibilità;
- procedere ad emissioni di assegni bancari e postali che rechino obbligatoriamente l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- la messa a disposizione di tutti i componenti del Consiglio di Amministrazione con congruo anticipo rispetto alla riunione programmata, (i) della bozza di bilancio, con idonea attestazione

dell'avvenuta consegna della stessa, nonché (ii) del giudizio sul bilancio da parte della società di revisione;

- predispongano, ove necessario, un programma di formazione di base rivolto a tutti i responsabili delle funzioni coinvolte nella redazione del bilancio e degli altri documenti equiparati, in merito alle principali nozioni e problematiche giuridiche e contabili, ivi inclusi corsi di aggiornamento periodici;
- con specifico riferimento al ciclo passivo relativo alla registrazione e pagamento delle fatture dei fornitori, le procedure prevedono:
  - la separazione tra la responsabilità di gestire le registrazioni contabili, di gestire i pagamenti e di assicurare le riconciliazioni dei flussi finanziari;
  - specifici controlli sull'impiego e la movimentazione delle risorse finanziarie;
  - l'autorizzazione dei pagamenti in funzione dei poteri vigenti in azienda;
  - specifici controlli supplementari per i pagamenti destinati a soggetti in Paesi ad elevato rischio terroristico;
  - che l'Ente Richiedente la fornitura attesti formalmente la prestazione eseguita/conformità merce e/o beni ricevuti ai fini dell'autorizzazione al pagamento della fattura;
  - l'amministrazione verifichi la presenza dei presupposti e delle necessarie autorizzazioni per il relativo pagamento (quali ad esempio l'esistenza di un OdA/Contratto di Acquisto, l'accettazione della prestazione da parte dell'Ente Richiedente, la congruenza tra importi e condizioni di pagamento riportate sull'OdA/Contratto e quanto indicato in fattura, ecc.);
  - i pagamenti ai fornitori devono essere effettuati a mezzo bonifico bancario su un conto corrente intestato al medesimo soggetto cui è conferito l'ordine/incarico, aperto presso un istituto di credito del paese di residenza/sede legale del soggetto cui è conferito l'incarico;
  - sono vietati pagamenti indirizzati a conti cifrati o a conti per i quali non si è in grado di individuare con precisione le generalità dell'intestatario;
  - tutti i pagamenti siano generalmente effettuati tramite bonifici bancari o comunque utilizzando esclusivamente mezzi di pagamento che consentano la tracciabilità dei flussi finanziari;
  - per tutti i tipi di pagamenti è vietato compiere operazioni tali da impedire la ricostruzione del flusso finanziario o da renderlo meno agevole quali, ad esempio, versamenti frazionati;
  - il divieto di cedere il credito a terzi salvo preventiva approvazione di Teleconsys;
  - il divieto per i terzi di chiedere pagamenti in Paesi diversi da quello ove viene svolta la prestazione ovvero abbia la sede il fornitore;
- con specifico riferimento al ciclo attivo relativo alla emissione e registrazione delle fatture attive ed alla gestione delle attività di tesoreria, le procedure prevedono che:

- sia garantita la separazione tra la responsabilità di richiedere l'emissione delle fatture attive e la responsabilità di gestire le correlate registrazioni contabili;
- sia garantita la separazione tra la responsabilità di gestire i flussi finanziari e la responsabilità di riconciliare contabilmente gli importi;
- gli incassi dei crediti verso i Clienti devono pervenire tramite istituto di credito presso il quale sia sempre possibile individuare il soggetto che ha disposto l'operazione verso la Società;
- tutti gli incassi siano generalmente gestiti tramite bonifici bancari o comunque utilizzando esclusivamente mezzi di pagamento che consentano la tracciabilità dei flussi finanziari e la loro provenienza;
- l'amministrazione analizzi gli aspetti contabili e amministrativi legati alla commessa nel rispetto delle indicazioni riportate nel contratto di vendita e nelle clausole contrattuali e archivi la documentazione ricevuta;
- la Società disponga di conti corrente presso primari Istituti di credito;
- i rapporti finanziari con le società partecipate siano gestiti attraverso l'utilizzo di c/c bancari.

Infine, oltre ai principi espressi nel Codice Etico, la Società prevede il divieto di:

- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio ricorrendo a fatture per operazioni inesistenti o alla sovra fatturazione), ovvero volte a creare "fondi neri" o "contabilità parallele";
- compiere operazioni personali, per conto proprio o per conto terzi anche per interposta persona, effettuate utilizzando informazioni acquisite in ragione delle proprie funzioni, nonché il divieto di raccomandare o indurre altri a compiere operazioni utilizzando le predette informazioni.

5.6. SISTEMI INFORMATIVI AZIENDALI

5.6.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Il processo di gestione dei sistemi informativi costituisce, in linea di principio, uno strumento attraverso il quale possono essere commessi alcuni tra i reati delle fattispecie previste dal D.Lgs. 231/2001, tra i quali si segnalano le false comunicazioni sociali, fatti di lieve entità, l'impedito controllo, la truffa e la corruzione. Devono, inoltre, considerarsi altri reati tipicamente legati all'ambiente informatico che potrebbero essere commessi in via astratta dalla Società, quali la frode informatica e quelli previsti dall'art. 24-*bis* (delitti informatici e trattamento illecito di dati) di seguito indicati:

- accesso abusivo ad un sistema informatico o telematico. Tale disposizione è rivolta a tutelare la riservatezza dei dati e dei programmi contenuti in un sistema informatico. La condotta rilevante consiste nell'introdursi abusivamente in un sistema protetto o nel permanervi contro la volontà espressa o tacita del titolare del diritto di escludere gli altri dall'uso del sistema. Oltre all'introduzione, rileva anche l'ipotesi del mantenersi in un sistema protetto contro la volontà espressa o tacita del titolare: tale caso ricorre quando in seguito ad un'introduzione involontaria o causale o solo inizialmente autorizzata, l'intruso permanga nel sistema informatico altrui, nonostante il dissenso del soggetto che ha interesse alla riservatezza dei dati e dei programmi in esso contenuti;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. Ai sensi della disposizione in esame la condotta può consistere alternativamente nell'intercettare fraudolentemente una comunicazione informatica o telematica, oppure nell'impedirla o interromperla. La condotta rilevante è quella che consente di intercettare una comunicazione informatica o telematica e cioè prendere cognizione del suo contenuto intromettendosi nella fase della sua trasmissione; l'intercettazione deve essere realizzata fraudolentemente, ossia eludendo eventuali sistemi di protezione della trasmissione in corso (ad es. decodificando dei dati trasmessi in forma cifrata o superando delle barriere logiche poste a difesa del sistema che invia o riceve la comunicazione) o, comunque, in modo tale da rendere non percepibile o riconoscibile a terzi l'intromissione abusiva;
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Tale disposizione mira a reprimere una condotta antecedente e preparatoria rispetto a quella prevista dalla precedente, vietando l'installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- danneggiamento di informazioni, dati e programmi informatici e danneggiamento di sistemi informatici o telematici. Oggetto del danneggiamento può essere innanzitutto un sistema informatico di qualsiasi tipo e dimensione eventualmente collegato a distanza con altri computer / apparecchiature come nel caso dei sistemi telematici. Oltre al sistema informatico, il danneggiamento può avere ad oggetto dati e programmi informatici. Le condotte rilevanti per l'illecito in esame sono la distruzione, il deterioramento e la inservibilità totale o parziale. L'ipotesi di distruzione di dati e programmi più frequente e significativa è rappresentata dalla loro cancellazione sia attraverso la smagnetizzazione del supporto, sia sostituendo i dati originari con dei nuovi dati dal contenuto diverso, sia impartendo all'elaboratore, in cui si trovano i dati o i programmi, uno dei comandi in grado di provocarne la scomparsa;

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. Il reato in esame è volto a punire la condotta di detenzione e di diffusione abusiva di codici di accesso che può portare alla commissione di altri reati informatici: infatti chi entra abusivamente in possesso di codici d'accesso, può commettere un accesso abusivo ad un sistema o può diffondere tali codici ad altre persone che a loro volta potrebbero accedere abusivamente al sistema. La disposizione in esame incrimina due tipi di condotte volte rispettivamente ad acquisire i mezzi necessari per accedere al sistema informatico altrui, oppure a procurare ad altri tali mezzi, o comunque, le informazioni sul modo di eludere le barriere di protezione;
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. Con tale principio si vuole tutelare il patrimonio informatico, inteso come hardware, software e dati da attacchi con virus informatici e malware. La condotta è la diffusione, la comunicazione o la consegna di un programma informatico che ha lo scopo o l'effetto di danneggiare il sistema informatico o telematico altrui, o di danneggiare dati o programmi in esso contenuti o ad esso pertinenti, oppure l'interruzione parziale o totale del suo funzionamento o la sua alterazione;
- falsità riguardanti documenti informatici. Tale principio fornisce una definizione di documento informatico basata sull'elemento materiale del supporto di memoria e non sui dati in esso contenuti. Le condotte penalmente rilevanti sono rappresentate dall'alterazione dei dati o delle informazioni riportate in un documento informatico o nella falsificazione del soggetto indicato come autore del documento.

Inoltre, non può escludersi il rischio correlato ad alcuni reati contemplati dall'art. 25 *novies* (delitti in materia di violazione del diritto d'autore), come di seguito illustrato:

- abusiva duplicazione, per trarne profitto, di programmi per elaboratore;
- predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori;
- 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.

Infine, le Società potrebbero potenzialmente incorrere nel reato di autoriciclaggio (art. 25-octies del D. Lgs.231/2001) se, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti non colposi di cui al D.Lgs. 231/01 ottengano delle utilità che impiegano, sostituiscono o trasferiscono, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

5.6.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalla Società come a potenziale rischio nella gestione dei sistemi informativi sono di seguito sintetizzate:

- definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico;
- gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione;
- gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni;

- gestione della sicurezza fisica (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni;
- acquisizione e gestione di apparecchiature, di dispositivi connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione);
- monitoraggio / verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica.

Occorre, inoltre, precisare che i reati informatici trovano come presupposto l'impiego di sistemi e programmi informatici. Al riguardo, è opportuno evidenziare che tutti i dipendenti aziendali che utilizzano ordinariamente sistemi informatici hanno conseguentemente ampia possibilità di accesso a strumenti e dati informatici e telematici nel contesto dell'ordinaria attività lavorativa. Per tale motivo, stante la capillare diffusione presso la Società di sistemi e strumenti informatici, si ritiene di valutare diffuso e non localizzato il rischio della loro commissione, infatti questi potrebbero essere astrattamente realizzati in ciascuna attività sensibile in capo alle diverse Funzioni/Aree delle Società.

5.6.3. PROTOCOLLI DI CONTROLLO SPECIFICI

In riferimento al processo di gestione ed utilizzo dei sistemi informativi, la Società adotta, anche attraverso adeguate clausole contrattuali con eventuali provider dei servizi IT, le seguenti *regole di condotta*:

- garantire l'acquisto e l'uso esclusivamente di software autorizzato e certificato;
- garantire che per installare software diversi da quelli messi a disposizione dalla Società sia necessario richiedere l'autorizzazione preventiva alla funzione Human Resource, Organization & IT;
- identificare formalmente un soggetto (Responsabile IT di sede) responsabile della gestione del sistema informativo aziendale, delle licenze software e della gestione dei rapporti con i consulenti IT esterni, ove incaricati;
- attribuire la funzione di Amministratore di Sistema previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità del soggetto individuato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di reati informatici, trattamento illecito dei dati, nonché rispetto della privacy;
- procedere al trattamento dei dati personali nel rispetto del principio di "accountability" (privacy by design e by default);
- compilare e mantenere aggiornato un inventario dell'hardware e del software in uso presso la Società;
- effettuare verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
- prevedere un piano di business continuity e disaster recovery;
- prevedere specifici criteri per l'assegnazione e la creazione, modifica e aggiornamento delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza);

- prevedere, nell'ambito della creazione e della assegnazione dei profili autorizzativi ai dipendenti, che la password di rete inizialmente creata di default dagli Amministratori di Sistema e assegnata ai dipendenti, sia conservata correttamente e cambiata periodicamente;
- prevedere il divieto assoluto di cedere e/o comunicare a terzi la password e creare identificativi facilmente decriptabili (es. nome-cognome del dipendente);
- garantire che le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti;
- definire i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- eseguire verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate e coerenti con i principi di segregazione dei ruoli, ove applicabili;
- archiviare la documentazione riguardante ogni singola attività allo scopo di garantire la completa tracciabilità della stessa;
- definire i criteri e le modalità per la gestione dei sistemi hardware e software che prevedano la compilazione e la manutenzione di un inventario aggiornato di apparati ed applicazioni in uso presso la Società e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware e/o software;
- definire i criteri e le modalità per le attività di back up che prevedano, per ogni applicazione hardware, la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;
- assicurare l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
- adottare sistemi idonei alla registrazione degli accessi mediante autenticazione informatica ai sistemi informatici e agli archivi elettronici da parte di tutti i dipendenti ivi inclusi gli Amministratori di sistema;
- impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzate per un determinato periodo di tempo, si blocchino automaticamente;
- dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- assicurare che l'utilizzo delle PEC aziendali sia limitato ai soli dipendenti all'uopo espressamente autorizzati, a cui è stata conferita un'adeguata rappresentanza della Società; in alternativa si suggerisce di far sottoscrivere alla/e risorsa/e che accede/no e che non hanno poteri di rappresentanza per la Società, una dichiarazione con la quale ci si impegna ad utilizzarla esclusivamente secondo le indicazioni di un procuratore aziendale.

Inoltre, *è fatto obbligo al personale dipendente ovvero ai collaboratori terzi che accedono ed utilizzano i sistemi informativi* della Società (Utenti) di rispettare le norme vigenti, le Regole Generali di Sicurezza emesse dalla Società, il Disciplinare Interno adottato ai sensi della normativa "Privacy" e di tutta le altre procedure e disposizioni al riguardo emesse da Teleconsys, ispirate ai seguenti principi di comportamento:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica;

- segnalare tempestivamente alle funzioni competenti il furto, il danneggiamento o lo smarrimento di tali strumenti;
- evitare di introdurre e/o conservare in Società (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 che siano stati acquisiti con il loro espresso consenso;
- evitare di trasferire all'esterno della Società e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio Personal Computer;
- evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa e formale autorizzazione dell'interessato;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici;
- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- aggiornare periodicamente le password, secondo le regole aziendali;
- non installare software/programmi aggiuntivi rispetto a quelli esistenti salvo quelli che verranno installati per esigenze aziendali;
- garantire la tracciabilità dei documenti prodotti;
- utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;
- in relazione alla casella di posta elettronica aziendale, limitarne l'utilizzo ai soli fini dell'attività lavorativa e assicurare la dovuta cautela nell'esposizione di concetti che potrebbero essere considerati presa di posizione ufficiale dell'azienda.

In relazione a quanto sopra ed in considerazione dei profili di natura prettamente tecnica della materia, al fine di supportare ed indirizzare gli Utenti ed il Responsabile IT di sede, a titolo esemplificativo ma non esaustivo, si riportano di seguito le principali fattispecie di violazioni, realizzate o anche solo tentate ovvero presunte tali, che devono essere segnalate all'O.d.V., anche in considerazione degli impatti effettivi o anche solo potenziali:

- introduzione in azienda di software non legale o punibile ai sensi della legislazione sul diritto d'autore;
- violazioni delle norme inerenti la privacy, la posta elettronica certificata e la firma digitale;
- tentativi di trasmissione di dati aziendali non autorizzati;
- tentativi di accesso non autorizzato ai sistemi informatici attraverso tecniche di hacking o escalation dei privilegi concessi;
- attacchi informatici o comportamenti non adeguati, provenienti dall'esterno (Internet) o dall'interno della network aziendale, finalizzati ad inibire parzialmente o completamente il servizio informatico;
- attacchi informatici o comportamenti non adeguati, provenienti dall'esterno (Internet) o dall'interno dell'azienda, finalizzati allo sfruttamento delle risorse IT per il compimento di reati informatici.

5.7. GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO E DELL'AMBIENTE

5.7.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO (SICUREZZA)

Le attività relative alla implementazione e gestione di sistemi di sicurezza e tutela dell'igiene dei luoghi di lavoro potrebbero originare illeciti di cui alle fattispecie previste dal D.Lgs. 231/01 art. 25-septies, in materia di sicurezza sul lavoro, vale a dire omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Affinché si origini la responsabilità di Teleconsys, è necessario non solo che si verifichi l'evento, ma occorre la "colpa specifica", ovvero che l'evento si sia verificato per l'inosservanza, a causa di condotta commissiva o omissiva cui è associabile un interesse o vantaggio dell'Azienda, delle norme per la prevenzione degli infortuni sul lavoro.

A titolo di esempio, potrebbero configurare un interesse o vantaggio di Teleconsys, in occasione di un evento che integra gli estremi dei reati di omicidio colposo o lesioni gravi o gravissime, le condotte poste in essere dalla Società in violazione della normativa per la prevenzione degli infortuni sul lavoro per conseguire risparmi sui costi di formazione, di consulenza e/o di servizi professionali legati alla salute e sicurezza sul lavoro, di manutenzione e monitoraggio degli ambienti di lavoro, di adeguamento antincendio, ecc..

Si evidenzia, infine, che i rapporti intrattenuti con pubblici ufficiali e/o incaricati di pubblico servizio nell'ambito delle attività a rischio riportate nel paragrafo successivo, in particolare con riferimento a verifiche cui Teleconsys può essere sottoposta o a richieste di autorizzazioni, rilevano anche ai fini dei reati di corruzione, istigazione alla corruzione, truffa o induzione indebita a dare o promettere utilità.

5.7.2. ATTIVITÀ A RISCHIO (SICUREZZA)

Il Documento di Valutazione dei Rischi ex D.Lgs 81/08 e s.m.i. (di seguito "DVR"), predisposto dalla Società in relazione ai luoghi di lavoro, individua le aree a rischio ai fini della prevenzione antinfortunistica e della tutela dell'igiene e della salute dei lavoratori.

Ferma restando l'individuazione e valutazione dei rischi di cui al DVR, di seguito si esplicitano le macro-attività individuate dalla Società come a potenziale rischio nell'ambito della salute e sicurezza nei luoghi di lavoro:

- gestione delle deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza;
- gestione del rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- gestione del processo di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione;
- gestione delle emergenze e primo soccorso e delle relative prove periodiche;
- gestione dei contratti d'appalto, d'opera o di somministrazione e della sicurezza nei cantieri temporanei o mobili;
- gestione delle riunioni periodiche della sicurezza e consultazione dei Rappresentanti dei Lavoratori per la Sicurezza;
- gestione del processo di formazione, informazione e addestramento;

- gestione della sorveglianza sanitaria e degli infortuni;
- gestione delle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte di lavoratori e verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate;
- gestione del processo di acquisizione di documentazione e certificazioni obbligatorie di legge.

5.7.3. PROTOCOLLI DI CONTROLLO SPECIFICI (SICUREZZA)

Oltre al rispetto dei principi espressi nel Codice Etico, è fatto obbligo ai Destinatari di:

- contribuire attivamente al mantenimento di uno standard ottimale di sicurezza, astenendosi da comportamenti illeciti o comunque pericolosi;
- attenersi scrupolosamente alle indicazioni fornite in materia di salute e sicurezza sui luoghi di lavoro dal personale preposto da Teleconsys, nonché presenti nel sistema documentale della Società, compreso il presente Modello;
- astenersi da comportamenti che possano mettere a rischio la propria ed altrui incolumità, segnalando tempestivamente al competente proprio superiore e al Servizio Prevenzione e Protezione ogni situazione di pericolo per la sicurezza propria o di terzi;
- seguire con diligenza la formazione in materia di salute e sicurezza erogata, direttamente o indirettamente, dalla Società.

È previsto l'espresso divieto a tutti i Destinatari di porre in essere, o anche tollerare che altri pongano in essere, comportamenti tali che considerati individualmente o collettivamente:

- possano compromettere i presidi di sicurezza adottati dalla Società favorendo potenzialmente la commissione dei reati di omicidio colposo e lesioni personali colpose;
- siano tesi ad impedire, intralciare, eludere, compromettere gli esiti dell'attività di vigilanza e controllo di sicurezza e igiene del lavoro, sia che essa sia svolta per conto della Società sia che sia svolta da autorità di controllo.

Nell'ambito del sistema interno di gestione della prevenzione e protezione dei lavoratori sui luoghi di lavoro, come da disposizioni di legge e normativa tecnica di settore:

- spetta al Datore di Lavoro di:
  - valutare i rischi per la sicurezza e salute dei lavoratori ed elaborare il "Documento sulla valutazione dei rischi" previsto dal D.Lgs. 81/08 con le modalità ivi prescritte;
  - designare il Responsabile del Servizio di Prevenzione e Protezione dai rischi;
- è fatto obbligo:
  - al **Datore di Lavoro,** al **Delegato del Datore di Lavoro** e ai **Dirigenti** ove presenti, in base alle funzioni conferite, nell'ambito delle loro aree di competenza e avvalendosi dei soggetti loro subordinati, nonché delle altre Funzioni o risorse di Teleconsys per loro disponibili, di rispettare quanto previsto dall'art. 18 del D.Lgs. 81/08;
  - ai **Preposti** ove presenti, nell'ambito delle loro attribuzioni e competenze, di rispettare quanto previsto dall'art 19 del D.Lgs. 81/08;

- ai singoli **Lavoratori**, di rispettare quanto previsto dall'art 20 del D.Lgs. 81/08;
- al **Servizio di Prevenzione e Protezione**, di attuare i compiti indicati all'art. 33 del D.Lgs. 81/08 avvalendosi della collaborazione del Datore di Lavoro o suo Delegato, dei Dirigenti, dei Preposti e del Rappresentante dei Lavoratori per la Sicurezza;
- al **Medico Competente**, di rispettare gli obblighi previsti dall'art. 25 del D.Lgs. 81/08;
- ai **Progettisti** dei luoghi e dei posti di lavoro e degli impianti, ai **Fabbricanti** e **Fornitori,** agli **Installatori e Montatori di impianti**, di rispettare quanto previsto rispettivamente dagli artt. 22, 23 e 24 del D.Lgs. 81/08.

Le attività connesse con il presente profilo di rischio devono altresì essere gestite nel rispetto della normativa applicabile e del sistema normativo interno che, oltre ad inglobare i principi espressi nel Codice Etico e gli obblighi e divieti sopra evidenziati, in relazione alle "attività a rischio" individuate prevede quanto segue:

- *gestione delle deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza:*
  - le nomine e le designazioni dei soggetti responsabili in materia di salute e sicurezza sul lavoro sono adeguatamente formalizzate, con firma da parte dei soggetti incaricati, e pubblicizzate all'interno della Società e all'esterno ove richiesto;
  - il sistema delle deleghe, nomine e designazioni è coerente con l'evoluzione dell'organizzazione della Società, garantisce la chiara identificazione dell'ambito di operatività delle deleghe nonché un flusso informativo formalizzato continuo/periodico tra delegante e delegato;
  - le persone incaricate di compiti rilevanti per la sicurezza sono dotate dei poteri di organizzazione, gestione e controllo, ed eventualmente di spesa, adeguati alla struttura ed alla dimensione dell'organizzazione ed alla natura dei compiti assegnati, in considerazione anche della possibilità del verificarsi di casi di urgenze non prevedibili né rinviabili;
  - sono definite le responsabilità e le modalità operative atte a garantire la verifica del possesso e del mantenimento dei requisiti di competenza e professionalità richiesti per le figure rilevanti per la sicurezza, con particolare riferimento ai requisiti di aggiornamento periodico obbligatori.

  Con particolare riferimento alla delega di funzioni da parte del Datore di Lavoro, come previsto dall'art. 16 del D.Lgs. 81/08, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni, che:
  - essa risulti da atto scritto recante data certa;
  - il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
  - essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
  - essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
  - la delega sia accettata dal delegato per iscritto.

Alla delega di funzioni deve essere data adeguata e tempestiva pubblicità. Essa non esclude l'obbligo di vigilanza in capo al Datore di Lavoro, da contemperare con il divieto di ingerenza, in ordine al corretto espletamento da parte del delegato delle funzioni trasferite.

Il soggetto delegato può, a sua volta, previa intesa con il Datore di Lavoro, sub delegare specifiche funzioni in materia di salute e sicurezza sul lavoro con i medesimi limiti e condizioni di cui sopra. La sub delega di funzioni non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale siano state sub delegate specifiche funzioni in materia di salute e sicurezza sul lavoro non può, a sua volta, delegarle ad altri.

In conformità a quanto previsto dall'art 17 del D.Lgs 81/08, il Datore di Lavoro non può delegare le seguenti attività:

- la valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'art. 28 del citato Decreto;
- la designazione del Responsabile del Servizio di Prevenzione e Protezione dai rischi;

- *gestione del rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici*. Sono formalizzati ruoli, responsabilità e modalità operative atte a garantire:
  - l'individuazione degli standard tecnico-strutturali di legge – applicabili a Teleconsys – riguardanti le attrezzature, gli impianti, i luoghi di lavoro, agenti chimici, fisici e biologici e il loro mantenimento nel tempo tramite adeguanti interventi di manutenzione ordinaria e straordinaria, programmata e a guasto. Nella programmazione delle attività di manutenzione e verifica periodica, si tiene conto di quanto previsto dalla normativa tecnica di settore, nonché delle informazioni contenute nei libretti d'uso e manutenzione delle singole apparecchiature, attrezzature, impianti;
  - l'esecuzione dei controlli periodici nei casi previsti dalla legge attraverso gli organismi pubblici o privati abilitati;
  - il rispetto dei principi generali di prevenzione in materia di salute e sicurezza sul lavoro al momento delle scelte progettuali e tecniche e nella scelta di attrezzature, componenti e dispositivi di protezione;
  - idonei flussi informativi tra il Servizio di Prevenzione e Protezione e le Funzioni a vario titolo coinvolte nel processo di approvvigionamento di beni e servizi, al fine di assicurare una gestione degli acquisti che tenga conto dell'esigenza di valutare preliminarmente i rischi che possono essere introdotti nella Società in fase di approvvigionamento;
- *gestione del processo di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione*. Il Datore di Lavoro, o suo Delegato per la parte relativa alla predisposizione delle misure di prevenzione e protezione, in collaborazione con il Servizio di Prevenzione e Protezione, il Medico Competente e previa consultazione del Rappresentante dei Lavoratori per la Sicurezza, provvede ad assicurare, per tutte le categorie di lavoratori e mansioni:
  - l'individuazione e valutazione di tutti i rischi per la sicurezza e la salute dei lavoratori, ivi compresi il rischio incendio e quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui quelli collegati allo stress lavoro-correlato, quelli riguardanti le lavoratrici in stato di gravidanza, nonché quelli connessi alle differenze di genere, all'età, alla

provenienza da altri Paesi e quelli connessi alla specifica tipologia contrattuale attraverso cui viene resa la prestazione di lavoro. Tale valutazione dovrà essere effettuata secondo le modalità e i contenuti previsti dagli artt. 28 e 29 del D.Lgs. 81/08;

- la redazione, a seguito della valutazione di cui al punto precedente, del DVR riportante i contenuti di cui all'art. 28 c. 2 del D.Lgs. 81/08 nel rispetto delle indicazioni previste dalle specifiche norme sulla valutazione dei rischi contenute nei successivi titoli del citato Decreto;
- l'aggiornamento periodico della valutazione di tutti i rischi secondo le modalità previste dagli artt. 28 e 29 del D.Lgs 81/08, avendo cura di garantire la coerenza tra l'evoluzione organizzativa di Teleconsys e il DVR;
- l'identificazione di misure idonee per prevenire, ove possibile, eliminare o comunque ridurre al minimo i rischi valutati, definendo le priorità d'intervento e pianificando i relativi interventi;
- l'eliminazione dei pericoli in relazione alle conoscenze acquisite e, ove ciò non fosse possibile, la riduzione di tali rischi al minimo con la predisposizione di idonee misure di prevenzione e protezione dei lavoratori in accordo con la seguente gerarchia:
    - sostituzione delle fonti di pericolo;
    - misure di controllo tecniche;
    - segnaletica e istruzioni e/o misure di controllo gestionale;
    - individuazione e dotazione di mezzi e dispositivi di protezione individuale;
- la valutazione ed il monitoraggio sull'applicazione delle misure adottate e la valutazione della loro efficacia;

- *gestione delle emergenze e primo soccorso e delle relative prove periodiche*. Sono formalizzati ruoli, responsabilità e modalità operative atte ad individuare le possibili emergenze e assicurare un'adeguata preparazione e risposta alle situazioni di emergenza mediante:
    - l'individuazione delle attività assoggettate agli adempimenti di prevenzione incendi e l'attuazione delle conseguenti misure di adeguamento;
    - l'individuazione delle possibili emergenze e la pianificazione delle relative modalità di gestione;
    - la designazione di 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. Il numero di incaricati designati all'emergenza è definito in considerazione della struttura organizzativa e operativa di Teleconsys, dell'eventuale presenza di disabili e delle possibili assenze degli incaricati per ferie/malattie/altro. Gli addetti, prima di essere adibiti a tali mansioni, sono adeguatamente formati ed addestrati. L'elenco degli addetti antincendio e primo soccorso viene reso noto a tutti i lavoratori;
    - l'organizzazione dei necessari rapporti con i servizi pubblici competenti in materia di primo soccorso, salvataggio, lotta antincendio e gestione dell'emergenza;
    - la definizione del piano di emergenza interno e la formalizzazione delle necessarie misure gestionali ed organizzative da attuare in caso di emergenza, affinché i lavoratori possano

cessare la loro attività, o mettersi al sicuro, abbandonando immediatamente il luogo di lavoro;

- l'informazione di tutti i lavoratori che possono essere esposti ad un pericolo grave e immediato e del personale esterno – es. ditte terze, visitatori - circa le misure predisposte e i comportamenti da adottare in caso di emergenza;
- la pianificazione ed esecuzione, nel rispetto della periodicità prevista dalla normativa di riferimento, di prove periodiche di emergenza ed evacuazione. Le prove di evacuazione vengono svolte congiuntamente ed in coordinamento con le altre realtà con le quali vengono eventualmente condivisi gli ambienti di lavoro. Viene inoltre garantita adeguata registrazione delle prove di emergenza e del processo di valutazione dei relativi risultati;
- la tempestiva rilevazione e comunicazione al Servizio di Prevenzione e Protezione e agli addetti alle emergenze, al verificarsi di un'emergenza, dei dipendenti e personale esterno presenti all'interno dei luoghi di lavoro. A seguito dell'evento dovrà essere garantita l'analisi delle cause e l'individuazione delle misure tecniche ed organizzative necessarie ad evitare il ripetersi di simili eventi;
- la presenza di planimetrie con l'indicazione delle vie di fuga e dei presìdi antincendio e di primo soccorso;
- la disponibilità di adeguati presidi di primo soccorso e di mezzi di estinzione idonei alla classe di incendio ed al livello di rischio presente sul luogo di lavoro, tenendo anche conto delle particolari condizioni in cui possono essere usati;

- *gestione contratti d'appalto, d'opera o di somministrazione e della sicurezza nei cantieri temporanei o mobili*. Sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - la selezione degli appaltatori, sia lavoratori autonomi sia imprese, previa verifica dell'idoneità tecnico professionale in conformità con quanto previsto dal D.Lgs. 81/08;
  - l'informazione, a fornitori e appaltatori, sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate;
  - la redazione del Documento Unico di Valutazione dei Rischi da Interferenza (di seguito "DUVRI") qualora i lavori ricadano nel campo d'applicazione dell'art. 26 del D.Lgs. 81/08, ovvero, nei casi previsti dallo stesso articolo, l'individuazione di un incaricato responsabile della cooperazione e del coordinamento. Nel DUVRI sono riportate le misure adottate per eliminare o ridurre al minimo i rischi da interferenze. In caso di redazione del documento, esso è allegato al contratto di appalto o di opera e ne è garantito l'adeguamento in funzione dell'evoluzione dei lavori, servizi e forniture;
  - l'attivazione delle procedure di cui al TITOLO IV del D.Lgs. 81/08 nel caso si tratti di cantieri temporanei e mobili;
  - l'indicazione, nei singoli contratti di subappalto, di appalto e di somministrazione, dei costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni;
  - l'indicazione, nei singoli contratti di subappalto, di appalto e di somministrazione, di specifiche clausole contrattuali con riferimento ai requisiti e comportamenti richiesti in

materia di salute e sicurezza, ed alle sanzioni previste per il loro mancato rispetto fino alla risoluzione del contratto stesso;

- che il controllo sugli adempimenti sia affidato ad un soggetto identificato e sia assicurata l'applicazione delle sanzioni (economiche, contrattuali);

- *gestione delle riunioni periodiche della sicurezza e consultazione del Rappresentante dei Lavoratori per la Sicurezza*. Sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - la consultazione del Rappresentante dei Lavoratori per la Sicurezza in tutti i casi previsti dall'art 50 del D.Lgs 81/08, garantendone adeguata tracciabilità;
  - lo svolgimento con periodicità almeno annuale di una riunione ex art. 35 del D.Lgs 81/08 cui partecipano il Datore di Lavoro o un suo rappresentante, il Responsabile del Servizio di Prevenzione e Protezione, il Medico Competente, il Rappresentante dei Lavoratori per la Sicurezza. Nel corso della riunione, di cui si conserva adeguata tracciabilità, vengono trattati almeno i seguenti argomenti:
    - il DVR;
    - l'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria;
    - i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale qualora necessari;
    - i programmi di informazione e formazione di dirigenti, preposti, lavoratori ai fini della sicurezza e della protezione della loro salute;

- *gestione del processo di informazione, formazione e addestramento*. Sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - un'adeguata informazione, formazione, addestramento dei lavoratori in conformità a quanto stabilito dagli artt. 36 e 37 del D.Lgs. 81/08 e dagli Accordi Stato-Regioni in materia di salute e sicurezza sul lavoro;
  - il possesso dei necessari requisiti da parte dei formatori della sicurezza in accordo a quanto definito dal Decreto interministeriale del 6 marzo 2013 e s.m.i.;
  - la tracciabilità dei processi di informazione, formazione, addestramento e verifica periodica dell'apprendimento;
  - un'adeguata informazione ai fornitori e agli appaltatori riguardo ai rischi specifici presenti nonché alle regole comportamentali e di controllo adottate da Teleconsys, definite nel presente documento e nel sistema normativo della stessa.

  Nel pianificare le attività di informazione, formazione, addestramento è fatto obbligo di considerare l'eventuale presenza di tirocinanti o apprendisti, lavoratori in distacco o distaccati, personale interinale, personale che effettua prestazioni occasionali di tipo accessorio.

  Nello specifico è previsto che ciascun lavoratore riceva una adeguata *informazione*:
  - sui rischi per la salute e sicurezza sul lavoro connessi alla attività aziendali in generale;
  - sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro;

- sui nominativi dei lavoratori incaricati di applicare le misure di primo soccorso e antincendio;
- sui nominativi del responsabile e degli addetti del Servizio di Prevenzione e Protezione, e del Medico Competente;
- sui rischi specifici cui è esposto in relazione all'attività svolta, sulle normative di sicurezza e le disposizioni di Teleconsys in materia;
- sui pericoli connessi all'eventuale uso delle sostanze e dei preparati pericolosi sulla base delle schede dei dati di sicurezza previste dalla normativa vigente e dalle norme di buona tecnica;
- sulle misure e le attività di protezione e prevenzione adottate.

Nello specifico è previsto che ciascun lavoratore riceva una formazione sufficiente ed adeguata in merito ai rischi specifici di cui al D.Lgs. 81/08. La *formazione* e, ove previsto, *l'addestramento* specifico avviene almeno in occasione:

- della costituzione del rapporto di lavoro o dell'inizio dell'utilizzazione qualora si tratti di somministrazione di lavoro e/o di prestazioni occasionali di tipo accessorio;
- del trasferimento o cambiamento di mansioni;
- dell'evoluzione dei rischi, dell'insorgenza di nuovi rischi o di modifiche legislative.

La normativa interna definisce ruoli, responsabilità e modalità operative per assicurare adeguata formazione, e i necessari aggiornamenti periodici, a particolari categorie di lavoratori, quali:

- Addetti al Servizio di Prevenzione e Protezione;
- Dirigenti e Preposti;
- Rappresentanti dei Lavoratori per la Sicurezza;
- lavoratori incaricati dell'attività di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;
- lavoratori esposti a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento;

- *gestione della sorveglianza sanitaria e degli infortuni*. La sorveglianza sanitaria viene garantita attraverso protocolli sanitari definiti dal Medico Competente sulla base dei rischi specifici. Nel pianificare le attività di sorveglianza sanitaria è fatto obbligo di considerare l'eventuale presenza di tirocinanti o apprendisti, lavoratori in distacco o distaccati, personale interinale, personale che effettua prestazioni occasionali di tipo accessorio. La periodicità dei controlli tiene conto della normativa applicabile nonché del livello dei rischi. Sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - la visita medica preventiva intesa a constatare l'assenza di controindicazioni al lavoro cui il lavoratore è destinato, al fine di valutare la sua idoneità alla mansione specifica;
  - la visita medica periodica per controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica;

- la visita medica su richiesta del lavoratore, qualora sia ritenuta dal medico competente correlata ai rischi professionali o alle sue condizioni di salute, suscettibili di peggioramento a causa dell'attività lavorativa svolta, al fine di esprimere il giudizio di idoneità alla mansione specifica;
- la visita medica in occasione del cambio della mansione, onde verificare l'idoneità alla mansione specifica;
- la visita medica alla cessazione del rapporto di lavoro nei casi previsti dalla normativa vigente;
- la visita medica preventiva in fase pre-assuntiva;
- la visita medica precedente alla ripresa del lavoro, a seguito di assenza per motivi di salute di durata superiore ai sessanta giorni continuativi, al fine di verificare l'idoneità alla mansione;
- l'aggiornamento tempestivo del protocollo sanitario, qualora dovesse rendersi necessario in relazione all'evolversi dell'organizzazione aziendale.

È fatto divieto di effettuare visite mediche per accertare stati di gravidanza e negli altri casi vietati dalla normativa vigente.

La cartella sanitaria e di rischio, istituita e mantenuta aggiornata per ogni lavoratore sottoposto a sorveglianza sanitaria a cura del Medico Competente, è custodita con salvaguardia del segreto professionale e della privacy presso il luogo concordato con il Datore di Lavoro o suo Delegato al momento della nomina.

Il sistema documentale aziendale definisce, inoltre, ruoli, responsabilità e modalità operative per garantire:

- una tempestiva comunicazione al Medico Competente in merito alle variazioni relative all'organico aziendale (es. assunzioni, cambio mansioni, cessazioni, rientri dopo malattie con assenze superiori ai 60 giorni, ecc.), affinché questi possa assicurare l'aggiornamento del calendario delle visite di idoneità e sorveglianza sanitaria;
- la vigilanza sull'assolvimento degli obblighi previsti per il Medico Competente, compresa la verifica periodica dei luoghi di lavoro;
- l'assolvimento degli obblighi di registrazione e comunicazione in caso di infortuni;
- l'analisi e monitoraggio degli infortuni compresi i "*near miss*";

- *gestione delle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori e verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate*. Sono definiti ruoli, responsabilità e modalità operative atte ad assicurare:
  - la vigilanza sul rispetto delle procedure e delle istruzioni di sicurezza da parte dei lavoratori e del personale esterno (es. fornitori, visitatori);
  - la segnalazione dei rischi rilevati e dell'eventuale mancato rispetto delle norme di sicurezza da parte dei lavoratori e del personale esterno;
  - l'applicazione del sistema disciplinare in caso di violazioni riscontrate;

- la pianificazione ed attuazione di verifiche periodiche e sistematiche dell'applicazione e dell'efficacia delle procedure adottate, anche con l'eventuale supporto di professionisti esterni formalmente incaricati nel rispetto delle regole comportamentali e di controllo definite nel presente Modello. Nella pianificazione delle attività di verifica si terrà conto di quanto risultante dalla Valutazione dei Rischi, della casistica relativa ad infortuni, incidenti e near miss, dei risultati delle attività di vigilanza e verifica periodica;
- la definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate nel corso delle verifiche;

- *gestione del processo di acquisizione di documentazioni e certificazioni obbligatorie per legge*. Sono definiti ruoli, responsabilità e modalità operative atte ad assicurare l'individuazione, l'acquisizione, la comunicazione l'aggiornamento, la conservazione e controllo, da parte delle varie Funzioni aziendali, ciascuna nell'ambito delle proprie responsabilità e competenze, della documentazione e delle certificazioni obbligatorie di legge o che la Società ritiene necessarie per un efficace gestione della salute e sicurezza sul lavoro.

5.7.4. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO (AMBIENTE)

Gli aspetti ambientali legati alle attività di Teleconsys presentano un profilo di rischio in quanto, in caso di gestione non conforme ai disposti legislativi applicabili in materia di ambiente, potrebbero originare illeciti di cui alle fattispecie previste dal D.Lgs. 231/01 art. 25-*undecies*.

Le tipologie di reato individuate come potenzialmente realizzabili sono:

- miscelazione di rifiuti pericolosi (art. 256 c. 5 DLgs 152/06). Il reato è astrattamente realizzabile nell'ipotesi di miscelazione, di rifiuti aventi caratteristiche di pericolosità diverse al fine di conseguire un risparmio sui costi di smaltimento;
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 c. 4 secondo periodo DLgs 152/06). Il reato è astrattamente realizzabile, anche in concorso con i fornitori/appaltatori per attività da questi svolta comunque sotto il controllo di Teleconsys, nell'ipotesi di predisposizione di un certificato di analisi, ove ne ricorra l'obbligo, che fornisce false indicazioni sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti;
- attività organizzate per il traffico illecito di rifiuti (art. 260 c. 1 DLgs 152/06)[2]. Il reato è astrattamente realizzabile in caso di cessione, ricezione, trasporto di rifiuti in difformità alla normativa applicabile ovvero avvalendosi di operatori terzi non autorizzati o che operano in difformità alle autorizzazioni e/o alla normativa applicabile;
- violazione delle disposizioni in materia di cessazione dell'utilizzo di sostanze lesive dell'ozono (art. 3 c. 6 L. 549/93). Il reato potrebbe realizzarsi, ad esempio, in caso di utilizzo di sostanze bandite oltre i termini previsti dalla legge;
- delitti colposi contro l'ambiente (452 quinquies c.p.). Il reato è astrattamente realizzabile nel caso in cui a seguito di una emergenza (es. incendio) derivante da condotta commissiva e/o omissiva, ne derivino compromissione o deterioramento significativi e misurabili ovvero alterazione irreversibile (o la cui eliminazione risulti particolarmente onerosa) dell'equilibrio

[2] Il D. Lgs n. 21 del 1/03/2018 con l'art. 7 ha abrogato, a partire dal 6/4/2018, l'art. 260 del D.Lgs 152/06 e s.m.i., inserendo il reato di "attività organizzate per il traffico illecito di rifiuti" all'art. 452 quaterdecies del c.p. e disponendo, mediante l'art. 8 del citato D.Lgs 21/2018, che "i richiami alle disposizioni abrogate dall'articolo 7, ovunque presenti, si intendono riferiti alle corrispondenti disposizioni del codice penale".

di un ecosistema, ovvero effetti lesivi su un elevato numero di persone o esposizione di un numero elevato di persone a pericolo;

- circostanze aggravanti (art. 452-*octies* c.p.). Il reato è astrattamente realizzabile nell'ipotesi di associazione a delinquere e associazione di tipo mafioso diretta, in via esclusiva o concorrente, allo scopo di commettere taluno dei delitti previsti nel titolo vi-bis del codice penale e associazione di tipo mafioso finalizzata all'acquisizione della gestione o comunque del controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi pubblici in materia ambientale. A titolo di esempio, potrebbe configurare un interesse o vantaggio dell'Azienda, in occasione di un evento che integra gli estremi dei reati di carattere associativo che determinano circostanze aggravanti, le condotte di associazione a delinquere tesa ad eludere, intralciare o impedire l'attività di vigilanza e controllo (ovvero la compromissione degli esiti dell'attività) per il tramite di negare l'accesso ai luoghi, per la predisposizione di ostacoli o in caso di mutamento artificioso dello stato dei luoghi.

Si evidenzia, infine, che i rapporti intrattenuti con pubblici ufficiali e/o incaricati di pubblico servizio nell'ambito delle attività a rischio riportate nel paragrafo successivo, in particolare con riferimento a verifiche cui Teleconsys può essere sottoposta o a richieste di autorizzazioni, ecc., rilevano anche ai fini dei reati di corruzione, istigazione alla corruzione, truffa o induzione indebita a dare o promettere utilità.

5.7.5. ATTIVITÀ A RISCHIO (AMBIENTE)

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della gestione ambientale sono di seguito sintetizzate:

- gestione dei rifiuti;
- gestione delle apparecchiature contenenti sostanze ozono lesive;
- gestione delle emergenze e attività soggette ai controlli dei VVFF.

5.7.6. PROTOCOLLI DI CONTROLLO SPECIFICI (AMBIENTE)

Oltre al rispetto dei principi espressi nel Codice Etico, è fatto obbligo ai Destinatari di:

- collaborare attivamente alla tutela e salvaguardia ambientale, astenendosi da comportamenti illeciti o comunque potenzialmente dannosi per l'ambiente;
- attenersi scrupolosamente alle indicazioni fornite in materia di tutela e salvaguardia ambientale dal personale preposto da Teleconsys, nonché presenti nel sistema documentale dell'azienda, compreso il presente Modello, segnalando tempestivamente al competente proprio superiore ogni situazione potenzialmente dannosa per l'ambiente;
- osservare tutti i dettami previsti dal D.Lgs. 152/06 e s.m.i. o da altre leggi e regolamenti in materia ambientale.

È previsto l'espresso divieto a tutti i Destinatari di porre in essere, o anche tollerare che altri pongano in essere, comportamenti tali che considerati individualmente o collettivamente:

- possano compromettere i presidi di tutela ambientale adottati dalla Società, favorendo potenzialmente la commissione dei reati ambientali di cui all'art. 25-undecies del D.Lgs. 231/01;

- siano tesi ad impedire, intralciare, eludere, compromettere gli esiti dell'attività di vigilanza e controllo ambientali sia essa svolta per conto della Società o da autorità di controllo.

In tema di deleghe di responsabilità e nomine/designazioni in materia di tutela dell'ambiente viene garantito che:

- le deleghe in materia ambientale, ove previste, sono adeguatamente formalizzate, con la specifica indicazione dei poteri delegati, la firma da parte dei soggetti incaricati, e pubblicizzate all'interno della Società e all'esterno ove richiesto;
- il delegato ambientale è in possesso di tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- il sistema delle deleghe, nomine e designazioni è coerente con l'evoluzione dell'organizzazione di Teleconsys, garantisce la chiara identificazione dell'ambito di operatività delle deleghe nonché un flusso informativo formalizzato continuo/periodico tra delegante e delegato;
- gli incaricati di compiti rilevanti per la tutela ambientale sono dotati dei poteri di organizzazione, gestione e controllo, ed eventualmente di spesa, adeguati alla struttura e alla dimensione dell'organizzazione e alla natura dei compiti assegnati, in considerazione anche della possibilità del verificarsi di urgenze non prevedibili né rinviabili.

Le attività connesse con il presente profilo di rischio devono essere gestite nel rispetto della normativa applicabile e del sistema normativo di Teleconsys che, oltre a inglobare i principi espressi nel Codice Etico e gli obblighi e divieti sopra evidenziati, prevede quanto segue:

- *gestione dei rifiuti*. Sono definiti ruoli, responsabilità e modalità operative atte a garantire:
  - il rispetto di tutti gli adempimenti previsti dalla normativa in capo al produttore del rifiuto, compreso il rispetto dei criteri di assimilabilità dei rifiuti stabiliti dal Comune di riferimento;
  - la tenuta del registro di carico/scarico ove ne ricorra l'obbligo;
  - il trasporto e smaltimento dei rifiuti speciali, ove ne ricorra l'obbligo, nel rispetto della normativa applicabile con particolare riferimento a:
    - affidamento dei rifiuti speciali a intermediari, trasportatori e smaltitori autorizzati;
    - verifica della correttezza e completezza della documentazione di trasporto;
    - monitoraggio del rientro della IV° copia del Formulario di Identificazione dei Rifiuti (FIR), nonché l'adozione dei provvedimenti di legge in caso di mancato rientro entro i tempi previsti dalla normativa;
  - l'inserimento, nei documenti contrattuali con appaltatori o subappaltatori operanti presso i siti aziendali, degli obblighi e divieti a loro carico in relazione alla gestione dei rifiuti da loro prodotti.

  Nell'ambito della gestione dei rifiuti è fatto divieto di:
  - miscelare rifiuti pericolosi con i rifiuti non pericolosi e rifiuti pericolosi che abbiano caratteristiche di pericolosità differenti;
  - effettuare trasporto in conto proprio di rifiuti;
  - effettuare spedizioni transfrontaliere di rifiuti ovvero, ove necessarie, effettuare tali spedizioni nel rispetto della normativa applicabile.

- *gestione delle apparecchiature contenenti sostanze ozono lesive*. Sono definiti ruoli, responsabilità e modalità operative atte a garantire:
  - il censimento degli impianti e apparecchiature contenenti sostanze ozono lesive con identificazione della tipologia e dei quantitativi delle sostanze in essi contenute;
  - la verifica che le sostanze presenti non rientrino tra quelle per le quali sono previsti divieti/restrizioni d'uso e eventuale dismissione degli asset e/o sostituzione delle sostanze vietate nel rispetto della normativa vigente;
  - l'aggiornamento periodico del censimento dei suddetti asset e la definizione di piani di manutenzione e verifica periodica nel rispetto della normativa vigente e mediante selezione di fornitori tecnicamente qualificati;
  - la tracciabilità di tutte le attività relative alla gestione di asset contenenti sostanze lesive dell'ozono.
- *gestione delle emergenze e attività soggette ai controlli dei VVFF*. Sono definiti ruoli, responsabilità e modalità operative atte a garantire:
  - l'individuazione delle tipologie di emergenza che possono cagionare danno all'ambiente e la predisposizione di adeguati presidi tecnici ed organizzativi per prevenire le emergenze e mitigarne gli effetti.

Oltre a quanto sopra, il sistema normativo di Teleconsys garantisce:

- un adeguato livello di informazione e, ove necessario, formazione dei dipendenti, sulle regole di comportamento in tema ambientale di Teleconsys e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole definite;
- un adeguato livello di informazione a fornitori e appaltatori, in merito alle regole di comportamento in tema ambientale di Teleconsys ed alle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole definite;
- l'attuazione di attività di vigilanza, anche con l'eventuale supporto di professionisti esterni formalmente incaricati nel rispetto delle regole comportamentali e di controllo definite nel presente Modello, con riferimento a
  - rispetto delle regole in materia ambientale anche da parte dei terzi che operano presso Teleconsys;
  - efficacia delle regole adottate;
  - conformità alla normativa ambientale delle attività;
- la definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate nel corso delle verifiche.

5.8. RAPPORTI CON I SOCI E LE SOCIETÀ PARTECIPATE

5.8.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

La gestione dei rapporti con i Soci e le Società partecipate potrebbe risultare strumentale alla commissione dei reati di corruzione, istigazione alla corruzione, di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, truffa, riciclaggio, ricettazione, nonché al concorso nella commissione dei reati di false comunicazioni sociali e fatti di lieve entità, ad esempio attraverso:

- la dazione o la promessa di somme di denaro a pubblici ufficiali o incaricati di pubblico servizio a fini corruttivi, servendosi dei Soci e/o delle Società partecipate;
- la dazione o la promessa di somme di denaro ad un rappresentante di una società controllata o ad un Socio per indurli a non rendere dichiarazioni o rendere dichiarazioni mendaci all'autorità giudiziaria;
- l'utilizzo di somme di provenienza illecita per la realizzazione delle attività con Soci o Società partecipate;
- l'intromissione dei Soci e/o delle Società partecipate nell'acquisto, nella ricezione o nell'occultamento di denaro o cose provenienti da un qualsiasi delitto;
- l'esposizione di fatti materiali non corrispondenti al vero;
- la contabilizzazione di poste fittizie e/o errate in tutto o in parte;
- l'omessa contabilizzazione di poste;
- la comunicazione alla PA di dati riguardanti le Società partecipate alterati/non veritieri.

Inoltre, tale area risulta potenzialmente a rischio anche della commissione dei reati di corruzione tra privati e istigazione alla corruzione tra privati, nel caso in cui un esponente della Società corrompa, ad esempio, un rappresentante di una società controllata o di un Socio, od offra o prometta a quest'ultimo denaro o altra utilità, per ottenere benefici non dovuti (es. contratto di vendita a condizioni fuori mercato, acquisizione di personale per diminuire il costo).

La Società potrebbe potenzialmente incorrere, altresì, nei reati di:

- indebita restituzione dei conferimenti, qualora vi sia la restituzione dei conferimenti ai Soci o la liberazione degli stessi dall'obbligo di eseguirli, in maniera palese o simulata, fuori dei casi di legittima riduzione del capitale sociale;
- illegale ripartizione degli utili o delle riserve, qualora vi sia la ripartizione di utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero la ripartizione riserve, anche non costituite con utili, che non possono per legge essere distribuite;
- illecite operazioni sulle azioni sociali o delle società partecipate, qualora si acquistino o sottoscrivano azioni o quote sociali, o della società controllante, che cagioni una lesione all'integrità del capitale sociale e delle riserve non distribuibili per legge.

Infine, la Società potrebbe potenzialmente incorrere nel reato di autoriciclaggio se, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti non colposi di cui al D.Lgs. 231/01, ottenesse delle utilità che successivamente fossero impiegate, sostituite o trasferite in attività economiche, finanziarie, imprenditoriali o speculative, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

5.8.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- Erogazione di servizi in favore delle Società partecipate;
- Acquisizione di beni e servizi da Soci e Società partecipate e gestione dei relativi contratti;
- Fatturazione e pagamenti tra le Società partecipate e tra Teleconsys e quest'ultime;
- Operazioni societarie che possono incidere sull'integrità del capitale sociale;
- Convocazione di CdA / Assemblea;
- Supporto nella predisposizione della documentazione per Consiglieri / Soci per le delibere poste all'ordine del giorno;
- Verbalizzazione delle riunioni di CdA / Assemblea e loro sottoscrizione;
- Decisioni del CdA;
- Decisioni dell'Assemblea dei Soci;
- Tenuta dei libri sociali;
- Gestione delle comunicazioni verso l'esterno.

5.8.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Con riferimento ai rapporti di natura commerciale (acquisizione e/o erogazione di servizi e gestione dei relativi contratti) con i Soci e le Società controllate, oltre a quanto indicato nel paragrafo 3.3 "*Regole di condotta nei rapporti con i terzi*", la Società si attiene alle seguenti regole di condotta:

- correttezza e trasparenza nei rapporti di natura commerciale con i Soci e le Società partecipate, nel rispetto del principio di autonomia degli stessi e dei principi di corretta gestione, trasparenza contabile, separatezza patrimoniale;
- definizione puntuale degli obblighi di comunicazione, tramite canali informativi formali, inerenti al perfezionamento di operazioni con i Soci e le Società partecipate;
- formalizzazione dei rapporti instaurati con le Società partecipate attraverso la sottoscrizione di specifici contratti;
- determinazione dei corrispettivi applicati alle operazioni commerciali e/o finanziarie intercorse con i soci azionisti di Teleconsys o con le Società partecipate secondo le "regole del mercato";
- gestione dei rapporti di natura commerciale (acquisti o cessioni di beni o servizi) con i Soci e le Società partecipate secondo i principi adottati con i terzi e comunque nel rigoroso rispetto della normativa applicabile senza alcun trattamento di favore o di agevolazione (es. collaudi, penali, ecc.);
- utilizzo, per quanto possibile, della contrattualistica e/o modulistica standard abitualmente adottata dalla Società nei rapporti con i terzi;
- tracciabilità di tutte le fasi del processo e archiviazione della documentazione rilevante (contratti, scambi di comunicazioni con i clienti/fornitori, ecc.) secondo le regole adottate dalla Società nei rapporti con i terzi.

Al fine di garantire la tutela del capitale sociale, la Società si attiene alle seguenti regole di condotta:

- agire con correttezza, trasparenza e collaborazione, nel rispetto delle norme di legge e delle procedure aziendali, al fine di garantire la tutela del capitale sociale;

- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- agire con correttezza, trasparenza e collaborazione nelle comunicazioni sociali, al fine di fornire ai Soci e agli altri destinatari delle informazioni societarie una rappresentazione corretta e veritiera della situazione patrimoniale, economica e finanziaria della Società.

5.9. RAPPORTI DI PARTNERSHIP ED RTI

5.9.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività aziendali (es. vendite, produzione, ricerca e sviluppo, ecc.) sulla base di Accordi di Partnership quali ad esempio le partecipazioni a Raggruppamenti Temporanee di Imprese (RTI), ecc. espone la Società, in via potenziale, alla commissione (anche in concorso) dei seguenti principali reati:

- corruzione e istigazione alla corruzione. Tali reati potrebbero essere commessi dal partner al fine di ottenere favori nell'ambito dello svolgimento delle attività commerciali e nella partecipazione alle procedure di selezione (es. gare) da parte della Pubblica Amministrazione (es.: promessa di denaro o altra utilità a Funzionario Pubblico al fine di acquisire ordini/contratti/varianti, ecc.);
- truffa. Tale reato potrebbe essere commesso attraverso la predisposizione di documentazione non veritiera, ad esempio tramite l'indicazione di aspetti tecnici non veritieri o di referenze non esistenti;
- induzione indebita a dare o promettere utilità. Tale fattispecie si configura, in via astratta, nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio induca un esponente dell'RTI a dargli o farsi promettere denaro o altra utilità, per ottenere un vantaggio non dovuto consistente nell'evitare l'adozione nei confronti della Società di un atto di per sé legittimo, ma dannoso o sfavorevole quale ad esempio un avviso di accertamento;
- corruzione tra privati e istigazione alla corruzione tra privati nel caso in cui un soggetto della Società per ottenere favori nell'ambito dello svolgimento delle attività in partnership tramite ad esempio la dazione o promessa di denaro o altra utilità ad un soggetto privato appartenente alla medesima partnership al fine di acquisire vantaggi e utilità;
- associazione per delinquere ed associazione di tipo mafioso, delitti di criminalità organizzata, nel caso in cui la Società ottenga il supporto di esponenti di associazioni delle tipologie suddette nell'aggiudicazione di appalti o contratti di fornitura (privati e/o pubblici) o, ad esempio mediante l'illegale fabbricazione e messa in vendita di prodotti, sistemi o soluzioni utilizzabili per scopi criminali.

Inoltre, considerando che generalmente le attività svolte in partnership rientrano nell'ambito dei processi ordinari della Società quali, ad esempio, le vendite, la produzione, la ricerca scientifica e tecnologica, ecc., non si possono escludere, in via teorica, anche ulteriori condotte illecite nella gestione delle partnership, riferibili a violazioni del D. Lgs. 231/2001, quali ad esempio i delitti con finalità di terrorismo o di eversione dell'ordine democratico, i delitti contro la personalità individuale, i reati di omicidio colposo e di lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, i reati ambientali, i reati di vendita di prodotti industriali con segni mendaci e di fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale.

5.9.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- studio delle opportunità/esigenze di partnership ai fini delle attività commerciali e di ricerca;
- individuazione e selezione dei potenziali partners;
- definizione e gestione degli accordi con i partners.

5.9.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La Società, ai fini dell'attuazione delle regole e dei divieti relativi alla gestione delle partnership, comprendente a titolo esemplificativo e non esaustivo, anche le fasi di individuazione delle opportunità e delle controparti, di definizione degli accordi, di ripartizione dei compiti e delle responsabilità e di rendicontazione delle attività, prevede le seguenti regole di condotta:

- i criteri di selezione dei Partner potenziali devono includere la verifica preventiva del possesso dei necessari requisiti di:
  - integrità;
  - lealtà;
  - correttezza;
  - trasparenza;
  - competenza;
  - professionalità.

  Nell'ambito degli accordi deve essere espresso il divieto di accettare o dare denaro od altra utilità o beneficio da parte o in favore dei Partner, che non trovi adeguata giustificazione e trasparenza nell'ambito del relativo rapporto;
- sia formalizzata l'attribuzione di poteri in capo ai responsabili della gestione dei rapporti con i soggetti predetti, distinguendo la fase d'instaurazione iniziale del rapporto dalle fasi di gestione;
- venga assicurata la trasparenza e la documentabilità delle attività realizzate (ad esempio, mediante compilazione di schede informative, la convocazione di apposite riunioni, la verbalizzazione degli incontri);
- gli accordi con i Partner sono definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso, in particolare per quanto concerne le condizioni economiche concordate. Tali accordi sono verificati ed approvati in base alle vigenti procedure e nel rispetto dei poteri conferiti. Nell'ambito di tali accordi deve essere reso palese che la violazione delle regole e dei principi di comportamento contenuti nel Codice Etico potrà determinare la risoluzione immediata del rapporto, salvo in ogni caso il maggior danno.

5.10. FINANZIAMENTI AGEVOLATI, CONTRIBUTI PUBBLICI ED AGEVOLAZIONI FISCALI A VARIO TITOLO

5.10.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

La gestione dei finanziamenti agevolati e dei contributi pubblici espone, in via potenziale, la società alla commissione dei reati di corruzione, istigazione alla corruzione, truffa aggravata per il conseguimento di erogazioni pubbliche, malversazione a danno dello Stato, indebita percezione di erogazioni a danno dello Stato e induzione indebita a dare o promettere utilità.

La corruzione si potrebbe verificare attraverso la promessa di denaro a funzionario pubblico al fine di acquisire i finanziamenti; la truffa aggravata si potrebbe realizzare attraverso la predisposizione di documentazione non veritiera in fase di ottenimento del finanziamento; la malversazione a danno dello Stato potrebbe verificarsi nel caso in cui la società muti la destinazione dei finanziamenti ricevuti per lo specifico fine della formazione utilizzandoli per la realizzazione di altre attività; l'indebita percezione di erogazioni a danno dello Stato potrebbe verificarsi nel caso in cui la Società riceva delle erogazioni di denaro o altri contributi senza averne titolo; infine l'induzione potrebbe configurarsi nel caso in cui un pubblico ufficiale o incaricato di pubblico servizio induca la Società a dargli o farsi promettere denaro o altra utilità per ottenere un vantaggio non dovuto (es. l'ottenimento di un finanziamento, l'anticipazione dell'erogazione di un finanziamento, la rendicontazione a fronte di documentazione non completa, ecc.).

Infine, la Società potrebbe potenzialmente incorrere nel reato di autoriciclaggio se, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti non colposi, ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

5.10.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- l'individuazione del contributo/finanziamento agevolato per l'attività di ricerca e sviluppo e relativa decisione di richiesta;
- l'individuazione dell'opportunità di avvalersi di agevolazioni fiscali e/o contributive;
- la preparazione della documentazione necessaria per ottenere il finanziamento, il contributo ovvero l'agevolazione;
- il monitoraggio dell'istruttoria dell'ente finanziatore e la stipula del contratto
- l'istruttoria e la determinazione della Pubblica Amministrazione per la concessione del contributo e/o agevolazione;
- la gestione del contratto di finanziamento agevolato o del contributo ovvero dell'agevolazione;
- la valutazione della possibilità di ottenere finanziamenti per l'attività formativa (Fondi Europei; Fondimpresa e Fondirigenti);
- l'erogazione dei corsi di formazione;
- la rendicontazione delle spese.

5.10.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La Società, ai fini dell'attuazione delle regole e dei divieti relativi alla gestione dei finanziamenti agevolati, dei contributi pubblici e delle agevolazioni fiscali, comprendente a titolo esemplificativo e non esaustivo, anche le fasi di individuazione delle opportunità, predisposizione e presentazione delle

domande, attuazione del progetto/iniziativa finanziata, rendicontazione delle attività e dei costi, incasso dei contributi, adotta i seguenti principi di controllo:

- deve essere predisposta una procedura per regolamentare tale attività a rischio che preveda:
  - le modalità di predisposizione delle domande di accesso al finanziamento, contributo o agevolazione, ovvero in generale della documentazione per ottenere i benefici richiesti o spettanti;
  - la corretta gestione delle risorse economiche acquisite
  - le modalità di rendicontazione interna ed esterna dell'utilizzo delle stesse;
  - la corretta gestione delle attività formative e relativa rendicontazione delle attività svolte.
- devono essere sviluppati appositi strumenti di controllo della veridicità e correttezza dei documenti prodotti per accedere a contribuzione e/o finanziamento e la successiva fase di rendicontazione tecnica ed economica;
- devono essere sviluppati specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- devono essere definiti con chiarezza e precisione ruoli e compiti all'interno della funzione responsabile del controllo della esatta corrispondenza tra il concreto utilizzo del contributo e/o finanziamento erogato ed il fine cui esso era destinato.

5.11. GESTIONE DEL PRE-CONTENZIOSO E DEL CONTENZIOSO

5.11.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

L'attività di gestione del pre-contenzioso e contenzioso (di qualsiasi natura esso sia, ovvero civile, penale, giuslavoristico, fiscale, ecc.) può comportare, in via teorica, il rischio di commissione dei reati di:

- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, attraverso ad esempio l'offerta o la promessa di denaro o altra utilità ovvero mediante atti di violenza o minaccia, nei confronti di una persona chiamata a rendere, davanti all'autorità giudiziaria, dichiarazioni utilizzabili in un procedimento giudiziario;
- corruzione in atti giudiziari ed istigazione alla corruzione, ponendo in essere un comportamento corruttivo (o un tentativo di comportamento corruttivo), sempre per favorire o danneggiare una parte in un processo civile, penale o amministrativo (ad esempio si corrompe un magistrato o un componente del collegio arbitrale, a titolo esemplificativo tramite l'intermediazione del legale di fiducia ovvero altro consulente/fornitore, per ottenere una pronuncia di condanna della controparte, in cambio, ad esempio, della promessa di una somma di denaro da accreditare su un conto intestato ad una Società o Ente estero facente capo al medesimo; oppure si corrompe un ausiliario di un magistrato per indurlo ad occultare un documento sfavorevole per Teleconsys, contenuto nel fascicolo del procedimento, in cambio, a titolo esemplificativo, del pagamento di una somma di denaro ovvero l'attribuzione di una consulenza a persona gradita all'ausiliario);
- truffa, alterando il contenuto della documentazione – in termini di incompletezza, non correttezza, ecc. – destinata al magistrato, al CTU o ad un componente del collegio arbitrale;
- induzione indebita a dare o promettere utilità, ad esempio nel caso in cui un pubblico ufficiale (Magistrato, ausiliario del Magistrato, ecc.), nell'ambito delle attività relative alla gestione di un contenzioso, induca la Società a dargli o farsi promettere denaro o altra utilità per ottenere una sentenza favorevole;
- corruzione tra privati e istigazione alla corruzione tra privati, nel caso in cui ad esempio un referente della Società dia o offra/prometta denaro o altra utilità non dovuta al legale ovvero al Consulente Tecnico della controparte per ottenere un vantaggio per Teleconsys.

5.11.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- individuazione dei legali esterni;
- sottoscrizione dell'incarico;
- gestione delle pratiche di pre-contenzioso e contenzioso e dei rapporti con i legali;
- approvazione di transazioni volte alla conclusione del contenzioso.

5.11.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La Società, oltre a quanto già previsto nel Codice Etico, prevede che i rapporti con la magistratura e con i pubblici funzionari che svolgono funzioni comunque connesse al contenzioso devono essere curati

esclusivamente dalle Direzioni/Funzioni competenti e devono essere improntati alla massima trasparenza, correttezza e collaborazione, evitando di esercitare ogni tipo di pressione o comunque di influenzare indebitamente le determinazioni di detti organi.

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto di quanto sopra e dei seguenti protocolli:

- la scelta dei legali e degli altri professionisti che supportano la Società nel contenzioso deve avvenire sulla base di criteri di serietà e competenza del professionista;
- i legali ed i professionisti dovranno prendere visione del Codice Etico e dichiarare di aderire ai principi in esso contenuti, tra cui l'assenza di situazioni di conflitto di interessi con la Società;
- l'attività prestata dai professionisti e dai legali deve essere debitamente documentata e la Direzione/Funzione che si è avvalsa della loro opera deve, prima della liquidazione dei relativi onorari, attestare l'effettività della prestazione;
- la corresponsione dei compensi ai professionisti ed ai legali esterni deve avvenire sulla base di una descrizione delle attività svolte, che permetta di valutare la conformità dell'onorario al valore della prestazione resa;
- deve essere garantita la tracciabilità, l'archiviazione e conservazione della documentazione relativa alla gestione dei contenziosi, con particolare riferimento a:
    - motivi che hanno portato all'apertura del contenzioso;
    - criteri per cui è stato selezionato il legale e la definizione;
    - strategia da adottare nel contenzioso;
    - decisione di accettare/proporre eventuali transazioni.

5.12. AFFARI SOCIETARI E RAPPORTI CON SOCIETÀ DI REVISIONE, COLLEGIO SINDACALE E SOCI

5.12.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività della presente area a rischio espone, in via potenziale, la Società alla commissione dei reati di:

- false comunicazioni sociali e fatti di lieve entità. Tali reati potrebbero configurarsi in via astratta attraverso l'effettuazione da parte del Consiglio di Amministrazione di azioni volte a predisporre un progetto di bilancio da proporre all'Assemblea dei Soci che contenga dati falsi ovvero che occulti aspetti rilevanti da portare all'attenzione dei Soci;
- indebita restituzione dei conferimenti. Il reato potrebbe astrattamente configurarsi nell'ipotesi in cui gli Amministratori delle Società restituiscano ai Soci conferimenti, fuori dei casi di legittima riduzione del capitale sociale e dai casi contemplati nello statuto;
- illegale ripartizione di utili e riserve. Tale reato potrebbe astrattamente configurarsi per la Società, a mero titolo esemplificativo, nei casi di:
    - ripartizione di utili o di 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 essere per legge distribuite, attuata ad esempio mediante la falsificazione, l'alterazione o la distruzione dei documenti di rendicontazione;
- operazioni in pregiudizio dei creditori. A mero titolo esemplificativo, tale reato potrebbe in concreto configurarsi nei casi di:
    - determinazione di poste valutative di bilancio non conformi alla reale situazione economica, patrimoniale e finanziaria delle Società;
    - esposizione in bilancio di altre poste (anche non valutative) inesistenti o di valore difforme da quello reale;
- formazione fittizia del capitale. Tale reato si potrebbe in astratto configurare laddove gli Amministratori ed i Soci conferenti provvedessero a formare/aumentare fittiziamente il capitale sociale ad esempio attraverso la sopravvalutazione in modo rilevante di conferimenti di beni in natura o di crediti;
- illecita influenza sull'assemblea. Tale reato si potrebbe in astratto configurare nell'ipotesi di simulazione o fraudolenta predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'Assemblea, anche in concorso con altri soggetti. Ad esempio, tale ultima fattispecie potrebbe concretizzarsi nel compimento di atti simulati o fraudolenti con cui si determina la maggioranza nell'Assemblea della Società;
- aggiotaggio. Tale reato si potrebbe in astratto configurare nell'ipotesi di diffusione di notizie e dati falsi effettuata con la finalità di alterare il prezzo di mercato di strumenti finanziari non quotati (ad esempio crediti o quote del capitale sociale delle Società);
- impedito controllo. Tale reato potrebbe in astratto essere realizzato nell'ipotesi in cui gli Amministratori e/o i loro diretti collaboratori occultino in tutto o in parte con mezzi fraudolenti informazioni/fatti che avrebbero dovuto essere comunicati al Collegio Sindacale riguardo la

situazione economica, patrimoniale o finanziaria della Società ovvero falsifichino/omettano delle comunicazioni/adempimenti nei confronti del Collegio Sindacale e/o dei Soci;

- autoriciclaggio nel caso in cui, a seguito della commissione o del concorso in commissione di un delitto non colposo tra quelli previsti nell'area a rischio in oggetto, si ottengano delle utilità da impiegare in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

5.12.2. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- partecipazione all'Assemblea dei Soci e/o gestione di adempimenti / predisposizione documentazione necessari per lo svolgimento dell'Assemblea dei Soci o da sottoporre all'Assemblea per la delibera;
- partecipazione al CdA e/o gestione di adempimenti / predisposizione di documentazione necessari per lo svolgimento dei CdA o da sottoporre al CdA per la delibera;
- effettuazione di operazione sul capitale sociale in virtù di delibere Assembleari/Consiliari;
- gestione dei rapporti con la Società di Revisione, con il Collegio Sindacale e con i Soci;
- gestione delle informazioni relative alla Società (ad es. tramite pubblicazioni sul sito internet aziendale, gestione delle relazioni con i media, ecc.).

5.12.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività relative alla presente attività a rischio devono essere gestite nel rispetto di quanto previsto nel Codice Etico e dei seguenti protocolli:

- divieto per i Destinatari di impedire od ostacolare in qualunque modo, anche occultando documenti o utilizzando altri idonei artifici, lo svolgimento delle attività istituzionali proprie dei Soci, del Collegio Sindacale e della società di revisione;
- i rapporti con i Soci devono essere gestiti garantendo parità di trattamento e di informativa e facendo in modo che le attività svolte non siano tese ad avvantaggiare un socio a discapito di altri;
- con riferimento ai rapporti con il Collegio Sindacale e la società di revisione:
  - i criteri e le regole seguite nella scelta della società di revisione devono essere formalizzati;
  - deve essere tenuta una riunione formale di apertura e chiusura delle attività di revisione;
  - l'eventuale affidamento di incarichi di consulenza alla società di revisione (ed alle società appartenenti al suo network) deve essere autorizzato dal Vertice Aziendale e deve essere formalizzato il motivo per cui si è fatto ricorso alla società di revisione e per cui si ritiene che l'affidamento dell'incarico non possa minare l'indipendenza di giudizio della società di revisione;

- tutti i dipendenti che entrano in contatto con tali organismi, sono tenuti ad informare tempestivamente il Responsabile della Funzione Administration, Finance & Control:
    - qualora si verificassero richieste da parte del Collegio Sindacale ovvero rilievi, problemi o eventi straordinari nella gestione dei rapporti con lo stesso;
    - in caso di richieste da parte della società di revisione;
- è fatto obbligo ai Destinatari di provvedere alla tempestiva:
    - trasmissione al Collegio Sindacale di tutti i documenti relativi ad argomenti posti all'ordine del giorno di Assemblee e C.d.A. o sui quali il Collegio debba esprimere un parere;
    - la messa a disposizione del Collegio Sindacale e della società di revisione dei documenti sulla gestione della Società per le verifiche proprie dei due organismi;
- la previsione di riunioni periodiche, o almeno in occasione della verifica annuale del Progetto di Bilancio, dell'O.d.V con il Collegio Sindacale e la società di revisione.

5.13. RAPPORTI NON COMMERCIALI CON LA PUBBLICA AMMINISTRAZIONE

5.13.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Preliminarmente all'analisi del potenziale profilo di rischio in merito ai rapporti con istituzioni ed enti pubblici, si evidenzia che, per la definizione di pubblico ufficiale ed incaricato di pubblico servizio, sono stati presi a riferimento per l'effettuazione del Risk Assessment e, più in generale, per la predisposizione del presente Modello, gli artt. 357, 358 e 322-bis c.p.; in particolare, gli articoli anzidetti riportano la nozione di *pubblici ufficiali* e di *incaricati di un pubblico servizio* italiani ed appartenenti ad organismi internazionali, come descritto al precedente paragrafo 3.2 della Presente Parte Speciale e di seguito illustrato:

1. *soggetti che svolgono una pubblica funzione legislativa o amministrativa*, quali, ad esempio:
   - parlamentari e membri del Governo;
   - consiglieri regionali e provinciali;
   - parlamentari europei e membri del Consiglio d'Europa;
   - soggetti che svolgono funzioni accessorie (addetti alla conservazione di atti e documenti parlamentari, alla redazione di resoconti stenografici, di economato, tecnici, ecc.);
2. *soggetti che svolgono una pubblica funzione giudiziaria*, quali, ad esempio:
   - magistrati (magistratura ordinaria di Tribunali, Corti d'Appello, Suprema Corte di Cassazione, Tribunale Superiore delle Acque, TAR, Consiglio di Stato, Corte Costituzionale, Tribunali militari, giudici popolari delle Corti d'Assise, giudici di pace, vice pretori onorari ed aggregati, membri di collegi arbitrali rituali e di commissioni parlamentari di inchiesta, magistrati della Corte Europea di Giustizia, nonché delle varie corti internazionali, ecc.);
   - soggetti che svolgono funzioni collegate (ufficiali ed agenti di polizia giudiziaria, guardia di finanza e carabinieri, cancellieri, segretari, custodi giudiziari, ufficiali giudiziari, testimoni, messi di conciliazione, curatori fallimentari, operatori addetti al rilascio di certificati presso le cancellerie dei tribunali, periti e consulenti del Pubblico Ministero, commissari liquidatori nelle procedure fallimentari, liquidatori del concordato preventivo, commissari straordinari dell'amministrazione straordinaria delle grandi imprese in crisi, ecc.);
3. *soggetti che svolgono una pubblica funzione amministrativa*, quali, ad esempio:
   - dipendenti dello Stato, di organismi internazionali ed esteri e degli enti territoriali (funzionari e dipendenti dello Stato, dell'Unione Europea, di organismi sopranazionali, di Stati esteri e degli Enti territoriali, ivi comprese le Regioni, le Province, i Comuni e le Comunità montane; soggetti che svolgano funzioni accessorie rispetto ai fini istituzionali dello Stato, quali componenti dell'ufficio tecnico comunale, membri della commissione edilizia, capo ufficio amministrativo dell'ufficio condoni, messi comunali, addetti alle pratiche riguardanti l'occupazione del suolo pubblico, corrispondenti comunali addetti all'ufficio di collocamento, dipendenti delle aziende di Stato e delle aziende municipalizzate; soggetti addetti all'esazione dei tributi, personale sanitario delle strutture pubbliche, personale dei ministeri, delle soprintendenze ecc.);
   - dipendenti di altri enti pubblici, nazionali ed internazionali (funzionari e dipendenti dell'Agenzia delle Dogane e dei Monopoli, della Banca d'Italia, delle Autorità di Vigilanza, degli istituti di previdenza pubblica, dell'ISTAT, dell'ONU, della FAO, ecc.).

Non sono considerate pubblico servizio le attività che, pur disciplinate da norme di diritto pubblico o da atti autoritativi, consistono tuttavia nello svolgimento di semplici mansioni di ordine o nella prestazione di opera meramente materiale (cioè attività di prevalente natura applicativa od esecutiva, non comportanti alcuna autonomia o discrezionalità o che prevedono unicamente il dispiegamento di energia fisica: ad esempio, operatore ecologico, dipendente comunale addetto alla sepoltura di salme).

La figura del pubblico ufficiale e dell'incaricato di pubblico servizio sono individuate non sulla base del criterio della appartenenza o dipendenza da un Ente pubblico, ma con riferimento alla natura dell'attività svolta in concreto dalla medesima, ovvero, rispettivamente, pubblica funzione e pubblico servizio.

Anche un soggetto estraneo alla pubblica amministrazione può dunque rivestire la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, quando eserciti una delle attività definite come tali dagli artt. 357 e 358 c.p. (ad esempio dipendenti di istituti bancari o notai ai quali siano affidate mansioni rientranti nel "pubblico servizio").

Passando ad analizzare il *potenziale profilo di rischio dell'area rapporti con le istituzioni ed enti pubblici*, la gestione dei rapporti con la Pubblica Amministrazione (di seguito anche "PA") espone la Società al rischio di commissione o concorso nei reati di:

- corruzione, ad esempio attraverso la dazione ovvero la promessa di denaro o di altra utilità a Funzionari della PA per non fare emettere provvedimenti/sanzioni nei confronti della Società;
- truffa in danno dello Stato, di altri enti pubblici o delle Comunità europee, ad esempio alterando il contenuto della documentazione – in termini di incompletezza, non correttezza, ecc. - destinata agli Enti Pubblici competenti in materia di personale appartenente alle categorie protette e truffa aggravata per il conseguimento di erogazioni pubbliche;
- induzione indebita a dare o promettere utilità nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio induca la Società a dargli o farsi promettere denaro o altra utilità per ottenere un vantaggio non dovuto, ad esempio la mancata applicazione di una sanzione;
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza ad esempio attraverso la predisposizione e l'invio alle autorità di vigilanza di documentazione non veritiera o l'occultamento e/o omissione di documenti ed informazioni rilevanti in sede di ispezioni.

Infine, la Società potrebbe potenzialmente incorrere nel reato di autoriciclaggio se, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti non colposi di cui al D.Lgs. 231/01, ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

5.13.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Le macro-attività individuate dalle Società, interessate come a potenziale rischio nell'ambito della presente area a rischio, esclusi i rapporti commerciali e di vendita di prodotti e servizi già esaminati nel paragrafo 5.1 "Attività commerciali e di vendita di prodotti/servizi" a cui si rinvia, sono di seguito sintetizzate:

- richieste di provvedimenti amministrativi occasionali necessari allo svolgimento delle attività aziendali;
- gestione delle visite ispettive a vario titolo da parte della PA (es. INPS, INAIL, GdF, ecc.);

- gestione dei rapporti con altre Autorità Ispettive (es. Garante Privacy);
- gestione dei rapporti con l'Autorità Giudiziaria ovvero con la Polizia Giudiziaria;
- invio e ricezione di documenti alla/provenienti dalla PA;
- gestione dei rapporti con Notai (nei casi svolgano attività di Pubblico Ufficiale).

5.13.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre ai principi espressi nel Codice Etico, la Società prevede l'obbligo di:

- svolgere le attività aziendali nel rigoroso rispetto dei limiti delle concessioni ottenute;
- portare all'attenzione del superiore gerarchico e/o dell'O.d.V. eventuali situazioni di incertezza in ordine ai comportamenti da tenere (anche in ragione dell'eventuale condotta illecita o semplicemente scorretta del pubblico agente), all'interpretazione della normativa vigente e delle procedure interne;
- inviare alle pubbliche autorità le segnalazioni previste dalla legge e dai regolamenti o richieste ad altro titolo alla Società in modo tempestivo, completo ed accurato, trasmettendo a tal fine tutti i dati ed i documenti previsti o richiesti;
- indicare nelle predette segnalazioni dati rispondenti al vero, completi e corretti, dando indicazioni di ogni fatto rilevante relativo alla situazione economica, patrimoniale o finanziaria della Società;
- utilizzare correttamente le procedure informatiche, tenendo conto delle più avanzate tecnologie acquisite in tale settore;
- per le attività connesse con le verifiche da parte della PA:
  - mettere a disposizione con tempestività e completezza la documentazione richiesta, garantendo la massima attendibilità delle informazioni fornite e la tracciabilità delle stesse;
  - garantire la massima disponibilità e collaborazione all'espletamento degli accertamenti ai quali possono partecipare esclusivamente dalle Direzioni/Funzioni competenti e delegate;
- seguire criteri di escalation gerarchica nella gestione dei diversi rapporti verso gli enti pubblici, soprattutto laddove si ravvisino criticità non risolvibili nell'ambito dell'ordinaria gestione;
- garantire la tracciabilità e l'archiviazione e conservazione della documentazione relativa ai principali rapporti intrattenuti con pubblici funzionari (ad esempio mediante scambio di email, redazione/sottoscrizione di verbali, comunicazioni tramite email al proprio superiore gerarchico di incontri tenuti con rappresentanti della PA).

5.14. OMAGGI, SPONSORIZZAZIONI, SPESE DI RAPPRESENTANZA ED INIZIATIVE PROMOZIONALI

5.14.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le eventuali iniziative della Società consistenti in omaggi, spese di rappresentanza, partecipazione ad eventi ed incontri di settore, sponsorizzazioni e pubblicità, costituiscono una modalità strumentale attraverso cui, in linea di principio, potrebbero essere commessi i reati di corruzione, di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, di corruzione tra privati e di istigazione alla corruzione tra privati.

La gestione anomala di tali attività potrebbe costituire, infatti, un potenziale supporto alla commissione dei reati suddetti, ad esempio, attraverso:

- la concessione di omaggi, liberalità, spese di rappresentanza, sponsorizzazioni a soggetti pubblici o assimilabili o a soggetti privati, per ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione amministrativa/contrattuale;
- la concessione di beni/servizi aziendali a titolo gratuito a soggetti pubblici o assimilabili o a soggetti privati, per ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione amministrativa/contrattuale;
- il riconoscimento di compensi ad agenzie per attività di promozione e di pubblicità per costituire fondi da utilizzare a fini corruttivi o al fine di indurre qualcuno a non rendere dichiarazioni o a renderne di mendaci all'autorità giudiziaria;
- la gestione anomala delle spese di rappresentanza quale potenziale strumento attraverso cui disporre di risorse finanziarie a fini corruttivi;
- la partecipazione ad eventi, incontri di settore gradite/i a soggetti pubblici o assimilabili o a soggetti privati, a fronte del pagamento di un corrispettivo fuori mercato, per ottenere in cambio ad esempio vantaggi, trattamenti di favore, mancata applicazione di una sanzione amministrativa/contrattuale.

Infine, la Società potrebbe potenzialmente incorrere nel reato di autoriciclaggio se, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti non colposi di cui al D.Lgs. 231/01, ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

5.14.2. ATTIVITÀ A RISCHIO

Nel presente paragrafo sono illustrate le analisi relative ad alcuni "processi sensibili" che risultano a rischio di commissione dei reati, anche se solo potenzialmente, in quanto caratterizzati, alla data di svolgimento del presente Risk Assessment, da un'attività operativa estremamente ridotta o del tutto assente.

Tuttavia, nell'ambito del profilo di rischio complessivamente considerato, non si può escludere che si possano determinare concrete fattispecie operative, al momento non prevedibili, ovvero uno sviluppo delle attività di seguito esaminate, con correlato rischio di commissione dei reati di cui al D. Lgs.231/2001. Pertanto, in via del tutto prudenziale, si è ritenuto opportuno rappresentare quanto segue sebbene in tutto o in parte non immediatamente riferibile e concretamente riscontrabile nell'ambito dei processi gestionali effettivamente in essere.

Le macro-attività individuate dalle Società interessate come a potenziale rischio nell'ambito della presente area a rischio sono di seguito sintetizzate:

- gestione omaggi;
- sponsorizzazioni;
- spese di ospitalità e rappresentanza;
- iniziative promozionali e partecipazione ad eventi.

5.14.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre a quanto espresso nel Codice Etico, la Società prevede che:

- gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore. In particolare, è vietato ricevere, pretendere, corrispondere ed offrire direttamente o indirettamente, compensi di qualunque natura, omaggi, vantaggi economici o altra utilità da/a un soggetto pubblico/privato che eccedano il modico valore e, comunque, siano suscettibili di essere interpretati come volti a influenzare indebitamente i rapporti tra la Società ed il predetto soggetto, a prescindere dalla finalità di perseguimento, anche esclusivo, dell'interesse o del vantaggio di Teleconsys;
- gli omaggi offerti o ricevuti devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- è fatto divieto di sostenere spese di rappresentanza e di ospitalità in favore di pubblici ufficiali o incaricati di un pubblico servizio o anche di privati, che possano influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società;
- i Destinatari devono garantire una adeguata tracciabilità della documentazione di supporto con riferimento agli omaggi effettuati ed alle spese di ospitalità e di rappresentanza.
- per le sponsorizzazioni o le iniziative promozionali la Società richiede:
    - specifiche procure, con limiti di importi;
    - la formale autorizzazione preventiva;
    - la valutazione formalizzata in un Report ex ante ed ex post, ove possibile, al fine di rilevare il ritorno economico e/o di "visibilità" in termini di immagine per la Società.