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

Modifiche approvate
dal Consiglio di Amministrazione
nella seduta del 22 Marzo 2023

Sommario

PARTE GENERALE 4

1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE 5
1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE 5
1.2. SANZIONI 6
1.3. DELITTI TENTATI 8
1.4. REATI COMMESSI ALL'ESTERO 8
1.5. PROCEDIMENTO DI ACCERTAMENTO DELL'ILLECITO E SINDACATO DI IDONEITÀ DEL GIUDICE 8
1.6. AZIONI ESIMENTI DALLA RESPONSABILITÀ 9
2. ADOZIONE DEL MODELLO DA PARTE DI TELECONSYS S.P.A. 10
2.1. OBIETTIVI E MISSION AZIENDALE 10
2.2. MODELLO DI GOVERNANCE 10
2.3. ASSETTO ORGANIZZATIVO E PARTECIPAZIONI 11
2.4. PRINCIPI GENERALI DI CONTROLLO 12
2.5. MOTIVAZIONI DELLA SOCIETÀ NELL'ADOZIONE DEL MODELLO 15
2.6. IL MODELLO ED IL CODICE ETICO 20
2.7. MODIFICHE ED INTEGRAZIONI DEL MODELLO 20
3. ORGANISMO DI VIGILANZA 20
3.1. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA 20
3.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA 23
3.3. INFORMATIVA DELL'ORGANISMO DI VIGILANZA NEI CONFRONTI DEGLI ORGANI SOCIALI 24
3.4. SEGNALAZIONI E FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 25
4. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO 27
4.1. FORMAZIONE DEL PERSONALE 27
4.2. INFORMATIVA AL PERSONALE 28
4.3. INFORMATIVA A COLLABORATORI ESTERNI E PARTNER 28
5. SISTEMA DISCIPLINARE 28
5.1. PRINCIPI GENERALI 28
5.2. SANZIONI PER I CONSIGLIERI DI AMMINISTRAZIONE 29
5.3. LE SANZIONI PER I DIPENDENTI CON QUALIFICA DI DIRIGENTE 29
5.4. LE SANZIONI PER I DIPENDENTI NON AVENTI QUALIFICA DI DIRIGENTE 30
5.5. LE SANZIONI PER I "TERZI DESTINATARI" 30
5.6. LE SANZIONI PER I SINDACI 31
5.7. LE SANZIONI PER L'ORGANISMO DI VIGILANZA 31
5.8. I COMPORTAMENTI SANZIONABILI E L'ACCERTAMENTO DELLE VIOLAZIONI 31
5.9. IL PROCEDIMENTO DI IRROGAZIONE DELLE SANZIONI 33

PARTE SPECIALE 35

1. FUNZIONE DELLA PARTE SPECIALE 36
2. LE REGOLE DI CONDOTTA 36
2.1. PRINCIPI GENERALI 36
2.2. REGOLE DI CONDOTTA NEI CONFRONTI DI ESPONENTI DELLA PUBBLICA AMMINISTRAZIONE 37
2.3. REGOLE DI CONDOTTA NEI RAPPORTI CON I TERZI 38
3. LA GESTIONE DELLE CRITICITÀ E SEGNALAZIONI ALL'ORGANISMO DI VIGILANZA 39
4. POTENZIALE PROFILO DI RISCHIO 39
4.1. FATTISPECIE DI REATO 40
5. LE AREE A RISCHIO REATO 58
5.1. ATTIVITÀ COMMERCIALI E DI VENDITA DEI PRODOTTI E SERVIZI 58
5.2. GESTIONE DEGLI ACQUISTI DI BENI E SERVIZI DA TERZI 62
5.3. REALIZZAZIONE COMMESSE, "DELIVERY" E SERVIZI 65
5.4. SISTEMI INFORMATIVI AZIENDALI 69
5.5. SELEZIONE, GESTIONE, FORMAZIONI ED AMMINISTRAZIONE DEL PERSONALE 75
5.6. AMMINISTRAZIONE, FINANZA, CONTROLLO ED OPERAZIONI SUL CAPITALE 79
5.7. GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO 91
5.8. AMBIENTE 100
5.9. RAPPORTI CON I SOCI, COLLEGIO SINDACALE E SOCIETÀ DI REVISIONE 103
5.10. ACCORDI, PARTNERSHIP, RTI CON TERZE PARTI 109
5.11. AREA LEGAL 111
5.12. OMAGGI, SPONSORIZZAZIONI, INIZIATIVE PROMOZIONALI E MARKETING 113
5.13. RAPPORTI NON COMMERCIALI CON LA PUBBLICA AMMINISTRAZIONE 115
6. RISK ASSESSMENT 117

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 aggiornamento, il presente documento è costituito dalle seguenti tipologie di condotte illecite, richiamate espressamente nel Decreto, come in ultimo aggiornato da:

- D.L. 124/2019, conv in Legge 157/2019 "Disposizioni urgenti in materia fiscale
- D.Lgs. 75/2020, recante "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" (c.d. "Direttiva PIF")
- Legge 9 marzo 2022, n. 22 "Disposizioni in materia di reati contro il patrimonio culturale"
- D.Lgs. 156/2022 "Disposizioni correttive e integrative del decreto legislativo 14 luglio 2020, n. 75, di attuazione della "Direttiva PIF"

- 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);
- art. 25-octies.1 (delitti in materia di strumenti di pagamento diversi dai contanti), aggiunto dal d.lgs. 184/2021;
- art. 25-quartedecies (reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati), introdotto dalla L. del 3 maggio 2019 n. 39;
- art. 25 - quinquiesdecies (reati tributari), introdotti dal Decreto Legge del 26 ottobre 2019, n. 124, convertito con L. 157/2019;
- art. 25 - sexiesdecies (reati di contrabbando), introdotti dal d.lgs.75/2020;
- art. 25 – septiesdecies (delitti contro il patrimonio culturale), introdotti dalla Legge 9 marzo 2022, n. 22;
- art. 25 – duodevicies (reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici), introdotti dalla Legge 9 marzo 2022, n. 22.

Dall'analisi delle suddette novità legislative si è valutato che le fattispecie contemplate dagli artt. 25-quartedecies, 25 - sexiesdecies, 25 – septiesdecies e 25 – duodevicies, recentemente introdotti, non rappresentano un rischio potenziale per TCS in quanto non vengono svolte attività aziendali che potrebbero, anche solo potenzialmente, esporre la Società alla commissione (anche in concorso) dei suddetti reati.

Altre fattispecie di reato potranno in futuro essere inserite dal legislatore nel Decreto Legislativo 231/01, con conseguente necessità di ulteriore 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

[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.

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..

1.4. 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:

1. il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;
2. l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
3. 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.
Con D.lgs. 4 ottobre 2022, n. 156 è stato modificato l' art. 25-quinquiesdecies 1-bis. In relazione alla commissione dei reati in materia di imposte sui redditi e sul valore aggiunto, previsti dal decreto legislativo 10 marzo 2000, n. 74, è stata estesa l'applicazione delle sanzioni laddove essi siano "commessi nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di Euro.
Sembrano pertanto interessare solo enti di grandi dimensioni e forza **economica e solo condotte fraudolenti su scala internazionale.**

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, successivamente integrate anche dal documento Confindustria "La responsabilità amministrativa degli enti ai tempi del COVID-19 Prime indicazioni operative Giugno 2020 e s.m.i.

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") è una Digital Innovation Company la cui missione è:

"*Supportare le organizzazioni pubbliche e private in tutte le fasi del loro viaggio di scoperta, adozione e evoluzione digitale, per aiutarle a cogliere le opportunità tecnologiche e di business che derivano dalle singolarità e dalle discontinuità dovute alle profonde trasformazioni in atto nei loro settori, ricorrendo all'adozione dei principali Digital Enabler, facendo leva sull'Open Innovation e ponendo costante attenzione ai temi della sostenibilità ambientale e sociale*".

La mission di Teleconsys è quindi quella di fungere da connettore per il mercato e per le amministrazioni pubbliche attraverso la Digital transformation e l'Industria 4.0, nella consapevolezza che, per essere sostenibile, la crescita e lo sviluppo devono essere in grado in grado di portare benessere alla società in toto, attraverso la condivisione della tecnologia.

La redazione del primo Bilancio di sostenibilità di Teleconsys, per il 2021, ha costituito un'importante opportunità per rappresentare ed evidenziare le linee strategiche di medio-lungo periodo e la loro coerenza con uno sviluppo sostenibile.

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.") 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.
- *Responsabile per la Protezione dei dati personali,* designato ai sensi di quanto previsto all'art. 37 del Regolamento (UE) 2016/679 (GDPR) svolge, in piena autonomia e indipendenza, i compiti e funzioni specificatamente richiamati nell'art. 39 del Regolamento.
- *Responsabile per la sicurezza nei luoghi di lavoro* designato ai sensi dell'art. 16 del D. Lgs. 9 aprile 2008 n. 81, assicura la corretta attuazione dei piani e programmi aziendali di prevenzione e protezione, così come definiti in attuazione del D. Lgs. 81/2008 e successive modifiche ed

integrazioni, e delle normative poste a tutela della sicurezza e della salute dei lavoratori durante il lavoro, ed in generale l'osservanza della normativa vigente in materia di ecologia e di tutela ambientale, da attuazione alla predetta disciplina, sia di fonte legale che derivante da norme di buona tecnica e di esperienza.

- *Organismo di Vigilanza (di seguito anche "O.d.V.")* cui è affidato il compito di vigilare sull'effettività e l'efficacia del funzionamento del Modello e delle procedure/Protocolli etico organizzativi che lo attuano, nonché di curarne gli aggiornamenti e la puntuale osservanza da parte di tutti quei soggetti ai quali le disposizioni del Modello e del Codice Etico sono dirette.

2.3. ASSETTO ORGANIZZATIVO E PARTECIPAZIONI

La struttura organizzativa dell'azienda adotta un modello definito come organizzazione matriciale debole che risponde alle necessità di attuare speditamente le linee strategiche di sviluppo del business e di definire una chiara attribuzione di obiettivi e responsabilità alle funzioni e alle unità operative (B.U.) e garantirne la separazione dei compiti (*segregation of duties*).

Agli inizi del 2021 Teleconsys ha rafforzato il suo modello di governance introducendo tre Comitati di seguito descritti.

- *Comitato di Direzione e Sostenibilità*

Il Comitato di Direzione e Sostenibilità presidia i meccanismi di coordinamento dell'azienda, gli orientamenti strategici e le relative linee guida attuative assicurando l'interscambio informativo tra le strutture ed i vertici aziendali. Il Comitato inoltre definisce, attua e verifica le politiche di sostenibilità dell'azienda.

Il Comitato di Direzione e Sostenibilità presidia e cura l'aggiornamento e il controllo delle principali decisioni e iniziative che hanno impatto sotto il profilo strategico e competitivo nel mercato di riferimento, con particolare attenzione agli aspetti di responsabilità sociale e sostenibilità dell'impresa di cui riferisce periodicamente al Consiglio di Amministrazione.

Per tutta la durata dello stato di emergenza nazionale, il Comitato ha anche avuto il compito di verificare la corretta applicazione delle regole contenute nel "Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro" adottato dall'Azienda.

Si riunisce mensilmente, entro la terza settimana del mese e comunque successivamente al Comitato Operativo.

- *Comitato Finanziario*

Il Comitato presidia la situazione finanziaria dell'azienda al fine di identificare, con sufficiente anticipo, possibili sofferenze ed attuare tutte le azioni necessarie a garantire la liquidità necessaria alla continuità e al sostegno del business, coerentemente con gli indirizzi di budget e con la strategia di pianificazione della struttura finanziaria.

- *Comitato Operativo*

Il Comitato monitora i principali indicatori economici e reddituali dell'azienda confrontandoli mensilmente con le previsioni di budget e di forecast al fine di identificare eventuali ritardi nel conseguimento degli obiettivi aziendali e attuare tutte le possibili iniziative per il raggiungimento delle performance attese.

Specifici Ordini di Servizio 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 tramite pubblicazione sulla intranet aziendale, assicurano la corretta individuazione degli ambiti di competenza di ciascuna struttura organizzativa all'interno dell'azienda.

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.

La società non è a capo né fa parte di un gruppo di imprese.

2.4. PRINCIPI GENERALI DI CONTROLLO

2.4.1. PROCEDURE E ORGANIZZAZIONE

Nello svolgimento delle attività aziendale, i soggetti interessati o coinvolti hanno innanzitutto l'obbligo di osservare le disposizioni di legge e i principi contenuti nel Codice Etico, nel Modello e Piano e nelle policy/procedure adottate dall'ente.
Sono adottati strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) orientati ad assicurare:

- una chiara formalizzazione e delimitazione dei ruoli, delle funzioni, delle responsabilità e dei livelli di autonomia (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 mediante pubblicazione sulla intranet aziendale);
- una chiara descrizione delle linee di riporto gerarchico;
- la conoscibilità, trasparenza e pubblicità dei poteri attribuiti (all'interno della Società e nei confronti dei terzi interessati);
- un'ampia diffusione e costante disponibilità all'interno dell'organizzazione dei corrispondenti documenti;
- standard comportamentali omogenei cui l'intera organizzazione deve conformarsi;

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

- separazione dei ruoli all'interno di ciascun processo (distinzione tra chi origina il processo, chi lo esegue, chi lo conclude e chi lo controlla);
- tracciabilità di ciascuna fase rilevante del processo e delle corrispondenti verifiche;
- adeguato livello di formalizzazione dei controlli eseguiti anche a livello di supervisione gerarchica;
- individuazione dei diversi livelli di approvazione e di ripartizione con segregazione dei compiti;
- sono formalizzate apposite procedure operative che regolano 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.

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.
Le modalità di gestione delle risorse finanziarie assicurano la separazione e l'indipendenza tra i

soggetti che concorrono a formare le decisioni di impiego delle risorse finanziarie, coloro che attuano tali decisioni e coloro ai quali sono affidati i controlli circa l'impiego delle risorse finanziarie.

Tutte le operazioni che comportano utilizzazione o impegno di risorse economiche o finanziarie devono avere adeguata causale ed essere documentate e registrate, con mezzi manuali o informatici, in conformità a principi di correttezza professionale e contabile. Il relativo processo decisionale deve essere verificabile.
Tutte le operazioni inerenti ad attività o prestazioni atipiche o inusuali devono essere specificamente e chiaramente motivate e comunicate all'Organismo di Vigilanza.
Le procedure organizzative sono aggiornate, anche su proposta o segnalazione dell'OdV stesso.

2.4.2. SISTEMA DI DELEGHE DI POTERI E DI FUNZIONI

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 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.
Ogni delega, formalizzata e consapevolmente accettata dal delegato, persona dotata di idonea capacità e competenza, prevede in termini espliciti e specifici l'attribuzione degli incarichi, assicurando al delegato l'autonomia ed i poteri necessari per lo svolgimento della funzione e specificando il soggetto (organo o individuo) cui il delegato riporta gerarchicamente.
L'organigramma aziendale, con l'indicazione delle funzioni attribuite a ciascuna posizione, è comunicato a tutti i dipendenti mediante pubblicazione sulla intranet aziendale e viene aggiornato in occasione di ogni sua variazione significativa.
Con riferimento alle attività relative ai processi a rischio, espressamente individuate nella Parte Speciale, il Modello 231 prevede specifici protocolli contenenti la descrizione formalizzata:

- delle procedure interne per l'assunzione e l'attuazione delle decisioni di gestione, con l'indicazione delle modalità relative e dei soggetti titolari delle funzioni, competenze e responsabilità, assicurando la separazione e l'indipendenza gerarchica tra chi elabora la decisione, chi la attua e chi è tenuto a svolgere i controlli;

- delle modalità di documentazione e di conservazione degli atti delle procedure in modo da assicurare la trasparenza e verificabilità delle stesse;

- delle modalità di controllo della conformità tra le procedure previste e la loro attuazione e documentazione.

Nel caso in cui siano previste modalità di rappresentanza congiunta è assicurato un principio di indipendenza gerarchica tra coloro che sono titolari del potere di rappresentanza in forma congiunta.

Deroghe ai protocolli ed alle procedure previsti nel Modello 231 sono ammesse in caso di emergenza oppure di impossibilità temporanea di attuazione delle stesse. La deroga, con l'espressa indicazione della sua ragione, è immediatamente comunicata all'Organismo di Vigilanza.

I protocolli sono aggiornati anche su proposta o segnalazione dell'OdV stesso.

2.4.3. SISTEMA DI CONTROLLO INTERNO

Il Sistema di Controllo Interno è costituito da un sistema procedurale, di governance e da norme più strettamente operative che regolamentano i processi aziendali, le attività ed i relativi controlli con l'obiettivo di assicurare:

- il rispetto delle strategie aziendali;
- l'efficacia ed efficienza dei processi;
- l'affidabilità e l'integrità delle informazioni contabili e gestionali;
- la conformità delle operazioni con la legge, i regolamenti e le procedure aziendali interne.

Il Sistema di Controllo Interno, periodicamente soggetto a monitoraggio ed adeguamento in relazione all'evoluzione dell'operatività aziendale e al contesto normativo di riferimento, si compone dei seguenti principali elementi:

- l'organizzazione aziendale formalizzata che definisce struttura, ruoli, responsabilità, poteri autorizzativi e dipendenze gerarchiche (l'organigramma aziendale è pubblicato sulla Intranet TCSpace);
- l'insieme delle procedure riferite ai diversi processi aziendali (le schede processo sono pubblicate sulla Intranet);

- gli ordini di servizio ed i regolamenti interni, pubblicati sulla Intranet, che disciplinano lo svolgimento delle attività interne ed assicurano la tracciabilità e documentabilità delle operazioni e dei controlli effettuati, nel rispetto del principio di separazione delle funzioni e di garanzia che ogni transazione o azione sia verificabile, documentata, coerente e congrua;

- un sistema di gestione delle risorse finanziarie e dei pagamenti, fondato sulle fasi di elaborazione del budget annuale e di analisi dei consuntivi periodici;

- un sistema di formazione ed informazione, volto alla sensibilizzazione e diffusione a tutti i livelli aziendali dei principi etici e delle regole comportamentali contenuti del Modello 231 integrato dal Codice etico e nel Bilancio di Sostenibilità;

- il Codice Etico, che racchiude i principi etici che devono essere osservati al fine di prevenire o ridurre i rischi di commissione di reato previsti dalla legge;

- un sistema disciplinare che interviene in caso di inosservanza delle disposizioni del Codice Etico, delle procedure operative e del Modello di organizzazione, gestione e controllo;

- un sistema di trasmissione e gestione delle denunce in conformità alla L. 179/17 (whistleblowing);

- un sistema di gestione dei processi certificato che soddisfa i requisiti delle seguenti norme internazionali per la Qualità:

ISO 9001:2015 Sistema di gestione della qualità

ISO 27001:2013 Sistema di gestione della sicurezza delle informazioni

ISO 27017:2015 Controlli avanzati di sicurezza nel cloud

ISO 27018:2019 Protezione delle informazioni personali nel cloud

ISO 20000-1:2018 Sistema di gestione dei servizi IT

ISO 45001:2018 Sistemi di gestione per la salute e sicurezza sul lavoro

ISO 14001:2015 Sistemi di gestione ambientale

2.5. 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".
Infatti, il 04 agosto 2022 Teleconsys ha ottenuto da parte dell'Autorità Garante della Concorrenza e del Mercato il **Rating di Legalità**, l'indicatore del rispetto di elevati standard di legalità da parte delle imprese, con il massimo punteggio ottenibile, pari a ★★★. Questo importante risultato colloca Teleconsys tra le aziende maggiormente impegnate ad adottare principi etici nei propri comportamenti e ad operare nel rispetto delle disposizioni di legge.

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.

2.5.1. *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.

Il Modello si pone come perno di un sistema di controllo e gestione dei rischi, **Teleconsys Enterprise Risk Management – TERMS,** integrata, secondo una proiezione unitaria, in tutte le attività dell'Organizzazione, a partire dal pensiero strategico dell'alta direzione nell'orientare la strategia del business alla crescita economica e di posizionamento sul mercato sino alle più elementari componenti delle attività progettuali ed operative. La gestione si basa sullo standard ISO 31000 e sul Framework Enterprise Risk Management del CoSO, al fine di garantire un processo standardizzato, ripetibile con risultati misurabili e confrontabili applicato a tutti i livelli dell'organizzazione.

2.5.2. *IL PROCESSO DI PREDISPOSIZIONE DEL MODELLO - PROCESSO DI ANALISI DEI RISCHI*

Teleconsys, al fine di dotarsi di un efficiente ed efficace Modello di organizzazione, gestione e controllo ha effettuato una serie di attività preparatorie suddivise in differenti fasi dirette alla costruzione e al periodico aggiornamento di un sistema di prevenzione e gestione dei rischi conforme con le disposizioni del Decreto e le Linee guida emanate da Confindustria (Ivi incluso il documento Confindustria La responsabilità amministrativa degli enti ai tempi del COVID-19 Prime indicazioni operative Giugno 2020 e s.m.i.).
Il Risk assessment è stato reiterato nel 2022, a fronte dei mutamenti avvenuti nel sistema organizzativo, all'implementazione delle fattispecie di reati che danno luogo alla responsabilità dell'Ente operata dal legislatore e all'implementazione delle procedure standard di controllo adottate dall'ente (ISO 45001, ISO 14001, Teleconsys Enterprise Risk Management - TERMS ISO 31000).
Di seguito si descrive l'approccio metodologico utilizzato per individuare le aree a rischio e definire il sistema dei presidi e dei controlli finalizzato alla prevenzione dei reati.
Il processo di analisi si è articolato secondo le seguenti fasi:

A. mappatura dei processi sensibili;
B. definizione e analisi dei rischi potenziali per singolo processo;
C. analisi, valutazione e adeguamento del sistema di controllo preventivo (c.d. protocolli).

A. Mappatura dei processi e valutazione del livello di presidio

È stata effettuata un'analisi della realtà aziendale (As is) al fine di censire le aree interessate alle potenziali casistiche di reato ed individuare i soggetti interessati all'attività di controllo e monitoraggio. Sulla base della documentazione aziendale disponibile (organigramma, disposizioni organizzative equivalenti, procedure, sistema di deleghe e procure, bilancio annuale), nonché della conoscenza della realtà aziendale, coadiuvata da interviste ai principali Referenti, è stata definita la mappa dei processi, delle strutture, delle responsabilità e delle procedure vigenti, nella quale sono elencati i processi individuati, l'attribuzione alle diverse strutture e sottostrutture organizzative, le procedure/istruzioni/policy che li descrivono, con l'indicazione di eventuali punti di attenzione e di eventuali esigenze di aggiornamento.
Il livello di presidio di un processo (e, all'interno di un processo, delle singole fasi/attività) viene valutato in funzione delle seguenti caratteristiche:

- procedure complete e formalizzate;
- presenza adeguati controlli e tracciabilità;
- responsabilità definite;
- esistenza deleghe e procure;
- segregazione delle funzioni.

B. Definizione e analisi dei rischi potenziali per singolo processo

1. INDIVIDUAZIONE DEI REATI APPLICABILI IN TELECONSYS S.P.A.

È stata effettuata una analisi dei reati previsti nel D.lgs. 231/01 e sono stati selezionati i soli reati le cui fattispecie sono concretamente applicabili alle attività svolte da Teleconsys.
In particolare sono stati esclusi i reati che, dopo una analisi preventiva, sono considerati non applicabili ovvero il cui rischio è stato considerato pressochè nullo in quanto la Società non svolge attività compatibili con la condotta materiale tipica del reato in esame ovvero non potrebbe avere interesse o

trarre vantaggio dalla commissione dello stesso. Per ciascun reato incluso sono state descritte le fattispecie rilevanti che possono concretamente verificarsi in Teleconsys, formulando casi esemplificative di condotte possibili.

2. DEFINIZIONE E ANALISI DEI RISCHI PER SINGOLO PROCESSO

Sono stati analizzati i singoli processi/fasi/attività e, per ciascuno di essi e per ciascuno dei reati applicabili, è stato valutato il livello di rischio.

Per la valutazione del livello di rischio conformemente agli standard diffusamente riconosciuti, si è tenuto conto dei due fattori:

- **Probabilità (P)** del rischio di commissione dei reati, stimata sulla base della possibile frequenza di accadimento nel contesto Teleconsys, in relazione ai singoli processi/fasi/attività oggetto di analisi.
- **Impatto (I)** valutato sulla base del possibile danno per Teleconsys derivante dalla commissione del reato, considerando sia il livello delle sanzioni amministrative pecuniarie ed interdittive legalmente previste a carico dell'ente, sia altri potenziali effetti dannosi sull'operatività aziendale derivanti dalla commissione del reato:

- possibile blocco o rallentamento dell'operatività aziendale;
- aggravi di tipo economico derivanti da perdite di contratti, applicazioni di penali, riduzione di efficienza nello svolgimento delle attività aziendali ecc.;
- danni reputazionali con impatto sull'organizzazione interna (perdita di personale) o sul proprio posizionamento sul mercato (capacità di acquisizione di nuove commesse, capacità di acquisizione di nuove linee di finanziamento o di mantenimento di quelle esistenti, deterioramento relazioni con clienti, partner o fornitori esistenti etc.);

segnalazione alle Autorità (ad es. ANAC, con conseguente esclusione dalla partecipazione a procedure di evidenza pubblica).

L'analisi dei rischi è riepilogata in una Matrice dei Rischi di reato, laddove R= P x I, strumento operativo di censimento, monitoraggio e controllo dei rischi aziendali in tema D.lgs. 231/01 (qui va inserito il Risk assessment TERMS).

C. Analisi, valutazione e adeguamento del sistema di controllo preventivo

Con riferimento al sistema dei presidi e controlli esistenti si è focalizzata l'analisi sulla presenza all'interno dello stesso dei seguenti elementi considerati essenziali:

- *Regole comportamentali:* esistenza di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi, dei regolamenti e dell'integrità del patrimonio aziendale.
- *Principi etici formalizzati*. Teleconsys ha predisposto 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. Le finalità di Teleconsys sono inoltre coerenti con i principi di un modello di sviluppo sostenibile e inclusivo, dove l'innovazione IT è al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale, come rappresentato nel primo Bilancio di sostenibilità di Teleconsys, redatto nel 2021.
- *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.

Sulla base della analisi dei rischi e della valutazione del livello di presidio dei processi sono state analizzate le procedure ed i controlli in essere al fine di valutarne l'adeguatezza e la eventuale necessità di integrazione o modifica, ossia la loro attitudine a prevenire comportamenti illeciti (o comunque a ridurne il rischio ad un livello accettabile) e ad evidenziarne l'eventuale commissione.
Quindi, per ciascuna area sensibile/processo sono stati valutati i seguenti elementi:

- i rischi di commissione di reato associati;
- il sistema dei presidi e controlli esistenti;

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.
A fronte di tale analisi e dei presidi e controlli individuati è stata poi effettuata una valutazione (Gap Analysis) dello scostamento tra la situazione in essere e quella ritenuta ottimale per assicurare un adeguato livello di presidio e quindi per il mantenimento del rischio ad un livello "accettabile", e sono state individuate le azioni necessarie di integrazione e/o miglioramento e i responsabili della loro attuazione nonché i termini previsti per la loro chiusura.

Nella Parte Speciale sono riportate, per ogni area/processo sensibile, le fattispecie di reato applicabili e le condotte esemplificative per la commissione di tali reati, la valutazione del livello di rischio, il sistema dei presidi e controlli (protocolli) esistenti.

2.6. 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.

2.7. 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 conoscenza effettiva dei contenuti del Modello e del Codice etico da parte delle risorse presenti in azienda e di tutti i soggetti che hanno rapporti con Teleconsys, è condizione necessaria per assicurare l'efficacia e la corretta funzionalità del Modello stesso.
La Società promuove pertanto 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 formazione ha l'obiettivo di diffondere tra il personale la conoscenza dei reati, le fattispecie configurabili, i presidi specifici delle aree di competenza degli operatori, nonché richiamare l'attenzione sull'importanza di una corretta applicazione del Modello. I contenuti formativi sono aggiornati in relazione all'evoluzione della normativa esterna e del Modello; pertanto in caso di modifiche rilevanti si procederà ad una integrazione dei contenuti medesimi, assicurandone altresì la fruizione.
La Società assicura la tracciabilità e le evidenze documentali della partecipazione dei dipendenti alla formazione sulle disposizioni del Decreto e sul Modello.
Ai neoassunti, nell'ambito del processo di inserimento nella Società, viene effettuata una specifica formazione, in modalità "e-learning" su supporto informatico, 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 e la pubblicazione sulla intranet aziendale delle 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:

- *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;
- *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.

2. LE REGOLE DI CONDOTTA

2.1. 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.

2.2. 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.).

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.

2.3. 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.

3. 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.

4. POTENZIALE PROFILO DI RISCHIO

4.1. FATTISPECIE DI REATO

La Parte Speciale si riferisce ai reati potenzialmente realizzabili all'interno di Teleconsys, di cui di seguito si descrivono brevemente, per una completa informativa, le singole fattispecie contemplate nel D.lgs. 231/2001 e s.m.i.

4.1.1. Reati commessi nei rapporti con la Pubblica Amministrazione e reati di concussione, induzione indebita a dare o promettere utilità e corruzione (artt. 24 e 25 D.lgs. 231/01)

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

Il reato si perfeziona quando chiunque, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalla UE.

Tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato (vedi *infra* art. 640 bis c.p.).

➢ ***Frode nelle pubbliche forniture (art. 356 c.p.)***

Tale ipotesi di reato si perfeziona nei casi in cui si commetta frode nell'esecuzione dei contratti di fornitura - sia di beni che di servizi - o nell'adempimento degli altri obblighi contrattuali nell'ambito di pubbliche forniture, ossia si adottino raggiri volti a ingannare la controparte ovvero venga modificata dolosamente l'esecuzione del contratto in danno alla controparte.

Affinchè si commetta il reato è necessaria sia presente la malafede contrattuale, ossia la presenza di un espediente malizioso o di un inganno, tali da far apparire l'esecuzione del contratto conforme agli obblighi assunti. E' richiesto anche un comportamento, da parte del fornitore, non conforme ai doveri di lealtà e moralità commerciale e di buona fede contrattuale.

➢ ***Truffa ai danni dello Stato (art. 640 c. 2, n. 1 c.p.)***

Il reato riguarda la condotta di colui che, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. In particolare, il fatto è commesso a danno dello Stato o di un altro ente pubblico.

La linea di demarcazione tra l'ipotesi di Truffa aggravata per il conseguimento di erogazioni pubbliche (ex art. 640 bis c.p.) e quella di Indebita percezione di erogazioni a danno dello Stato (ex art. 316 ter c.p.) risiede nel tipo di condotta criminosa del reo che, nel secondo caso, si limita a presentare documenti falsi o ad omettere informazioni dovute; mentre nella prima ipotesi pone in essere artifizi o raggiri che provocano l'induzione in errore della Pubblica Amministrazione.

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

La pena è aggravata e si procede d'ufficio se il fatto di cui all'articolo 640 c.p. (Truffa) riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o dell'UE.

Tale fattispecie può realizzarsi nel caso in cui gli artifici o raggiri si sostanzino nella comunicazione di dati non veri o nella predisposizione di una documentazione falsa, per ottenere finanziamenti pubblici o erogazioni pubbliche.

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

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico. Il reato è aggravato nel caso di realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, ovvero laddove la Società rivesta la qualità di operatore del sistema.

SANZIONI

- sanzione pecuniaria fino a 500 quote.
- sanzioni interdittive:

c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

e) il divieto di pubblicizzare beni o servizi.

➢ ***Corruzione (art. 318, 319 c.p.)***

Tale reato si configura quando il pubblico ufficiale, o l'incaricato di pubblico servizio indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente).

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

Tale ipotesi di reato si configura nel caso in cui un soggetto, parte di un procedimento giudiziario, al fine di ottenere un vantaggio nel procedimento stesso corrompa un pubblico ufficiale (magistrato, cancelliere od altro funzionario).

Il reato in esame potrebbe realizzarsi in concreto, laddove un soggetto apicale o eterodiretto ponesse

➢ ***Concussione (art. 317 c.p.)***

Tale ipotesi di reato si perfeziona quando un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della propria qualità o dei suoi poteri, costringa taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altre utilità non dovutegli.

Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.lgs. 231/2001; in particolare, tale forma di reato può ravvisarsi solo nell'ipotesi di concorso nel reato del pubblico ufficiale di un dipendente della Società (e sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).

Va evidenziato, inoltre, che tale reato potrebbe esser commesso anche da un soggetto aziendale **in danno della Società** e non a vantaggio della stessa (e quindi che sia carente il presupposto richiesto per l'ascrivibilità all'ente ai fini della 231).

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

Il reato si realizza quando il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Valgono le osservazioni svolte per il reato di concussione.

Il d.lgs. 75/2020 è intervenuto sull'art. 25 del d.lgs. n. 231/2001, ampliando il panorama dei delitti contro la P.A., che ora comprende i reati di **peculato** di cui agli **artt. 314 e 316 c.p.** e il delitto **di abuso**

di ufficio di cui all'**art. 323 c.p.** Rispetto a tali fattispecie di reato, l'estensione della responsabilità alle persone giuridiche risulta tuttavia circoscritta, in accoglimento delle osservazioni all'uopo formulate dalla II Commissione permanente della Camera dei deputati nella seduta del 20 maggio 2020, ai soli casi in cui «il fatto offende gli interessi finanziari dell'Unione europea».

SANZIONI

- sanzione pecuniaria: artt. 318, 321, 322, co. 1 e 3, e 346-bis c.p.: 200 quote;
  artt. 319, 319-ter, co. 1, 321, 322, co. 2 e 4, c.p.: 200 - 600 quote;

  artt. 317, 319 c.p. quando dal fatto l'ente ha conseguito un profitto di rilevante entità: 300 - 800 quote.
- sanzioni interdittive: per una durata non <4 e >7, se il reato è stato commesso da apicale e per una durata non <2 e >4 , se il reato è stato commesso da un sottoposto.

DIVIETI GENERALI

Con riferimento ai reati contro la PA menzionati al paragrafo 4.1.1. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- firmare atti o documenti che abbiano rilevanza esterna alla Società in assenza di poteri formalmente attribuiti;
- destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi, o finanziamenti, a scopi diversi da quelli per cui sono state concesse;
- corrispondere od offrire, direttamente o indirettamente, anche sotto forme diverse di aiuti o contribuzioni, pagamenti o benefici materiali a pubblici ufficiali o incaricati di pubblico servizio per influenzare o compensare un atto del loro ufficio ed assicurare vantaggi di qualunque tipo alla Società;
- accordare altri vantaggi di qualsiasi natura, effettuare promesse o indebite elargizioni di denaro o altra utilità a pubblici funzionari o incaricati di pubblico servizio o persone a questi ultimi vicini;
- dare seguito a richieste indebite di denaro o altri benefici provenienti da qualunque persona. In tali casi, il dipendente deve informare tempestivamente il proprio superiore e sospendere ogni rapporto d'affari con il richiedente;

• cedere a raccomandazioni o pressioni provenienti da pubblici funzionari o incaricati di pubblico servizio;

• tenere condotte ingannevoli nei confronti della Pubblica Amministrazione tali da indurre quest'ultima in errori di valutazione nel corso dell'analisi di richieste di autorizzazioni e simili;

• omettere informazioni dovute, al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione;

• presentare dichiarazioni non veritiere a organismi pubblici, ad esempio esibendo documenti incompleti e/o non corrispondenti alla realtà;

• porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa, nel corso di processi civili, penali o amministrativi;

• utilizzare denaro contante come mezzo di pagamento e incasso, al di fuori dei casi consentiti dai regolamenti e dalle procedure aziendali o comunque in modo improprio;

• effettuare pagamenti non adeguatamente documentati e autorizzati;

• effettuare pagamenti o riconoscere compensi in favore di soggetti terzi, senza adeguata giustificazione contrattuale o altra giustificazione;
• effettuare assunzioni di personale non meritocratiche, favorendo soggetti "vicini" o "graditi" a pubblici ufficiali o incaricati di pubblico servizio;
• assumere personale senza aver adottato un iter di selezione trasparente e criteri meritocratici nella valutazione dei candidati;
• selezionare personale ovvero favorire l'avanzamento interno di carriera o il riconoscimento di premi per il raggiungimento di obiettivi a beneficio di taluni dipendenti, non ispirandosi a criteri strettamente meritocratici o in base a criteri di valutazione non oggettivi;
• riconoscere rimborsi spese in favore di dipendenti, collaboratori o terzi che non trovino adeguata giustificazione in relazione al tipo di incarico svolto o in assenza di idonea documentazione giustificativa;
• erogare forme diverse di aiuti o contribuzioni che, sotto veste di sponsorizzazioni, abbiano invece la finalità di promuovere o favorire interessi della Società, anche a seguito di illecite pressioni;
• promettere o versare omaggi o liberalità al di fuori dei limiti e delle modalità definiti nel Codice Etico e nel protocollo specifico di seguito riportato;
• attribuire utilità aziendali a soggetti appartenenti alla Pubblica Amministrazione per ottenere in cambio comportamenti illeciti favorevoli per la Società;
• promettere o versare indebitamente somme o beni in natura a qualsiasi soggetto per promuovere o favorire gli interessi della Società;
• instaurare rapporti o porre in essere operazioni con soggetti qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione di uno o più reati.

4.1.2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis D.lgs. 231/01)

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

Il delitto potrebbe essere commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), ad esempio, per prendere cognizione di dati riservati di un partner commerciale, di una stazione appaltante o di un competitor.

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

Il reato in parola si realizza nel caso in cui si intercettino, impediscano o interrompano comunicazioni informatiche o telematiche, ovvero se ne rilevino il contenuto, mediante qualsiasi mezzo di informazione al pubblico. L'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, o comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

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

La fattispecie di reato in questione si considera integrata, con vantaggio dell'ente, nel caso in cui, ad esempio, un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato, si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

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

La condotta in esame potrebbe realizzarsi laddove soggetti apicali della Società ponessero in essere attività di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici, e ciò eventualmente anche al fine di agevolare o coprire una propria condotta illecita.

➢ ***Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)***

Questo delitto si distingue da quello di cui al precedente punto poiché in questo caso il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità.

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

Questo delitto si distingue da quello di cui ai precedenti punti poiché in questo caso il danneggiamento ha ad oggetto sistemi informatici o telematici.

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

Questa fattispecie criminosa si configura quando i sistemi informatici o telematici sono "di pubblica utilità" (cd. "attentato al sistema").

SANZIONI

- sanzione pecuniaria: 100 - 500 quote
- sanzioni interdittive: a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi.

➢ ***Falsità in documenti informatici (art. 491-bis c.p.)***

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

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

SANZIONI

- sanzione pecuniaria: 400 quote
- sanzioni interdittive: a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi.

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

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

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

Questi fatti sono punibili solo nel caso in cui il soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento dei sistemi o dei dati.

Tali condotte sarebbero aggravate laddove realizzate su sistemi informatici sui quali la Società o gli addetti della Società rivestano la qualifica di "Amministratori di sistema".

SANZIONI

- sanzione pecuniaria: 300 quote
- sanzioni interdittive: b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi.

DIVIETI GENERALI

Con riferimento ai delitti informatici menzionati al paragrafo 4.1.2. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- utilizzare le risorse informatiche (es. personal computer fissi o portatili) assegnate per finalità diverse da quelle lavorative;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
- acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
- danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
- utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- distruggere o alterare documenti informatici archiviati sulle directory di rete o sugli applicativi aziendali se non espressamente autorizzati, e in particolare i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- utilizzare o installare programmi diversi da quelli autorizzati dalla Direzione Sistemi Informativi;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (antivirus, firewall, proxy server, ecc.);
- lasciare il proprio personal computer sbloccato e incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- utilizzare in modo improprio gli strumenti di firma digitale assegnati;

- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio alla Società;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o in supero dei diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze).

4.1.3. DELITTI DI CRIMINALITÀ ORGANIZZATA (art. 25 ter D.lgs. 231/01)

➢ ***Associazione per delinquere (art. 416, escluso comma 6 c.p.)***

Tale delitto è configurabile in tutti i casi in cui tre o più persone si associno allo scopo di commettere più delitti, tra quelli mappati nel presente Modello, rilevanti ai fini del D.lgs. 231/01, ovvero anche al fine di commettere reati che non siano ricompresi nel catalogo dei reati presupposto dal D.lgs. 231/01.

SANZIONI

- sanzione pecuniaria: 400 -1000 quote
- sanzioni interdittive, per una durata non inferiore ad un anno

DIVIETI GENERALI

Per la sua natura particolare, caratterizzata da una carenza di tipicità della fattispecie, il reato di "associazione per delinquere" è astrattamente configurabile in tutti gli ambiti di attività della Società caratterizzati da un contatto frequente o continuativo con terze parti, laddove uno o più soggetti interni alla Società, approfittando delle proprie mansioni, possano associarsi con soggetti anche esterni al fine di commettere in forma organizzata più delitti nell'interesse o a vantaggio della Società. Conseguentemente, **c**on riferimento al reato di associazione a delinquere menzionato al paragrafo 4.1.3. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, in tutte quelle attività che comportano rapporti stabili e continuativi con soggetti terzi, è fatto espresso divieto di:

- adottare comportamenti che risultino pregiudizievoli per l'integrità, l'autonomia o l'immagine della Società;
- promettere o versare indebitamente somme o beni in natura a qualsiasi soggetto per promuovere o favorire gli interessi della Società condizionare, anche indirettamente, la concorrenza o il mercato;
- comunicare a terzi informazioni riservate sulla Società;
- riconoscere compensi in favore di fornitori, consulenti, o altri collaboratori senza adeguata giustificazione e in assenza di accordi formalizzati;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di denaro;
- instaurare rapporti o porre in essere operazioni con soggetti qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione di uno o più reati;
- erogare servizi fittizi, non necessari, a prezzi non definiti sulla base delle policy aziendali, allo

scopo di determinare redditi imponibili non corretti/veritieri o di creare fondi utilizzabili per scopi corruttivi;

- effettuare dichiarazioni dei redditi non rispondenti a quanto risultante dalla contabilità o in generale effettuare operazioni atte a determinare un reddito imponibile non corretto / veritiero.

4.1.4. FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (art. 25 bis D. Lgs. 231/2001)

➢ ***Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (Art. 473 c.p.)***

Tale delitto è configurabile in tutti i casi in cui, potendo conoscere dell'esistenza del titolo di proprietà industriale, qualcuno contraffi o alteri marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque senza essere concorso nella contraffazione o alterazione, faccia uso di tali marchi o segni contraffatti o alterati. La pena è aggravata laddove l'azione delittuosa abbia ad oggetto brevetti, disegni o modelli industriali, nazionali o esteri.

SANZIONI

- sanzione pecuniaria: 500 quote
- sanzioni interdittive, per una durata non inferiore ad un anno

4.1.5. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (art. 25 bis-1 D.lgs. 231/01)

➢ ***Turbata libertà dell'industria o del commercio (art. 513 c.p.)***

➢ ***Frode nell'esercizio del commercio (art. 515 c.p.)***

Il delitto si configura laddove, nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico, il venditore consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.

➢ ***Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)***

Il delitto si configura nel caso in cui si ponga in vendita o si mettano altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.

➢ ***Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)***

Si tratta di ipotesi residuali rispetto a quella contemplata nell'art. 473 c.p.
Elementi rilevanti ai fini della punibilità sono:

- potenziale conoscenza dell'esistenza di un titolo di proprietà industriale,
- fabbricazione o utilizzo industriale, ovvero vendita con offerta diretta ai consumatori o messa in circolazione di beni con segni mendaci o realizzati usurpando titoli di proprietà industriale
- introduzione nel territorio dello Stato o detenzione per la vendita dei beni di cui al punto precedente.

SANZIONI

- sanzione pecuniaria: fino a 500 quote

➢ ***Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)***

Le condotte, integranti la fattispecie di cui all'articolo 513 c.p. sono state ritenute dalla giurisprudenza nelle seguenti:

- Uso di violenza sulle cose, che si realizza ogni qualvolta la cosa venga trasformata, danneggiata o ne venga mutata la destinazione
- Ricorso a mezzi fraudolenti (atti di concorrenza sleale Art. 2598 c.c.) quali:
  - Pubblicità menzognera
  - Pubblicità denigratoria
  - Uso di altrui marchi registrati
  - Concorrenza parassitaria
  - Boicottaggio
  - Storno di dipendenti
  - Rifiuto di contrattare
  - Inserimento nel codice sorgente del proprio sito internet di parole chiave direttamente riferibili alla persona, impresa o prodotto di un concorrente

➢ ***Frodi contro le industrie nazionali (art. 514 c.p.)***

Tale delitto è configurabile in tutti i casi in cui qualcuno, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagiona un documento all'industria nazionale. Questa ipotesi, peraltro, dà rilievo non solo ai marchi e segni distintivi registrati secondo la normativa nazionale od internazionale, ma anche a quelli che non lo sono, sancendo, quindi, un'ampia protezione del bene tutelato.
Se per i marchi o segni distintivi sono state osservate le norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà industriale, la pena è aumentata.

SANZIONI

- sanzione pecuniaria: fino a 800 quote
- sanzioni interdittive

DIVIETI GENERALI

Con riferimento ai reati contro l'industria e il commercio menzionati al paragrafo 4.1.5. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- attuare comportamenti violenti o intimidatori o condizionare le attività commerciali, industriali o produttive di terzi con forme di intimidazione tipiche della criminalità organizzata, al fine di ostacolare/eliminare la concorrenza;
- compiere atti di concorrenza sleale, ed in particolare:
  - diffondere notizie e apprezzamenti sui prodotti e/o sull'attività di un concorrente, idonei a determinarne il discredito, o appropriarsi di pregi dei prodotti o dell'impresa degli stessi;
  - avvalersi direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale ed idoneo a danneggiare l'altrui azienda;
- consegnare ovvero utilizzare beni o servizi differenti da quanto dichiarato o pattuito con i clienti, atti a indurre in inganno lo stesso sull'origine, la provenienza, la qualità o la quantità del bene / servizio, tra cui la data di produzione, il numero di ore lavorate;
- porre in essere atti di violenza sulle cose di terzi (es. danneggiare o trasformare beni di

terzi/concorrenti).

4.1.6. REATI SOCIETARI (ART. 25 TER D.LGS. 231/01)

➢ ***False comunicazioni sociali e false comunicazioni sociali in danno della società, dei soci e dei creditori (artt. 2621 e 2621-bis c.c.)***

Il reato in esame potrebbe configurarsi nel caso in cui amministratori, apicali, o sindaci, ovvero il preposto al bilancio, espongano nelle comunicazioni sociali previste dalla legge fatti materiali rilevanti non rispondenti al vero, ovvero omettano fatti materiali rilevanti la cui comunicazione è imposta dalla legge.

- sanzione pecuniaria: 200 - 400 quote

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

Il reato in esame potrebbe realizzarsi nel caso in cui gli amministratori impediscano o comunque ostacolino lo svolgimento delle attività di controllo legalmente attribuite ai soci o agli altri organi sociali.

- sanzione pecuniaria: 100 - 180 quote

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

Sono puniti gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

- sanzione pecuniaria: 100 - 180 quote

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

Il delitto in esame potrebbe configurarsi in caso di ripartizione di utili o conti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero di ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite.

- sanzione pecuniaria: 100 - 130 quote

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

Sono puniti gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

- sanzione pecuniaria: 100 - 180 quote

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

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

- sanzione pecuniaria: 150 - 330 quote

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

Il reato in esame potrebbe configurarsi nel caso in cui gli amministratori e i soci conferenti formino o aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, mediante sottoscrizione reciproca di azioni o quote, oppure attraverso una sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti o del patrimonio della società nel caso di trasformazione.

- sanzione pecuniaria: 100 - 180 quote

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

Il delitto in esame potrebbe configurarsi nel caso in cui la società fosse posta in liquidazione, laddove fossero poste in essere operazioni che cagionino danno ai creditori, mediante ripartizione di beni sociali tra i soci prima di avere estinto più obbligazioni verso i creditori o di avere accantonato le somme necessarie a soddisfarli. IL reato è punibile anche a titolo di concorso.

- sanzione pecuniaria: 150 - 330 quote

➢ ***Corruzione ed istigazione alla corruzione tra privati (art. 2635-bis c.c.)***

Il reato in esame potrebbe compiersi laddove gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori della Società ricevano, nello svolgimento di un'attività privatistica, denaro o altra utilità, ovvero laddove i medesimi soggetti offrano denaro o altra utilità ai soggetti sopra elencati di altre società private. Il reato è profilabile anche per interposta persona e senza che necessariamente sia cagionato nocumento alla società.

- sanzione pecuniaria: 400 - 600 quote
- sanzioni interdittive

➢ ***Istigazione alla corruzione tra privati (art. 2635 bis c.c.)***

- sanzione pecuniaria: 200 - 400 quote
- sanzioni interdittive

➢ ***Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza (art. 2638 c.c.)***

Il reato in esame potrebbe realizzarsi nel caso in cui gli amministratori, ovvero i soggetti apicali della Società ovvero gli addetti agli organi di controllo, pongano in essere condotte di ostacolo all'esercizio delle funzioni delle Autorità di Vigilanza, ad esempio al fine di evitare alla Società sanzioni o altre conseguenze pregiudizievoli.

- sanzione pecuniaria: 200 - 400 quote

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

Il reato potrebbe realizzarsi nel caso in cui gli amministratori determinino la maggioranza in assemblea in modo fraudolento, allo scopo di procurare un profitto o un vantaggio per la Società, ad esempio al fine di garantire la continuità aziendale.

- sanzione pecuniaria: 150 - 330 quote

➢ ***Aggiotaggio (art. 2637 c.c)***

Delitto commesso da chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione di strumenti non quotati,

- sanzione pecuniaria: 200 - 500 quote

DIVIETI GENERALI

Con riferimento ai reati societari menzionati al paragrafo 4.1.6. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- rappresentare in contabilità - o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali - dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società e delle sue controllate;
- registrare in contabilità operazioni a valori non corretti rispetto alla documentazione di riferimento, oppure a fronte di transazioni inesistenti in tutto o in parte, o senza un'adeguata

documentazione di supporto che ne consenta in primis una corretta rilevazione contabile e successivamente una ricostruzione accurata;

- omettere dati ed informazioni previsti dalla normativa vigente o dalle procedure interne sulla situazione economica, patrimoniale e finanziaria della Società e delle sue controllate;
- restituire conferimenti al Socio o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale previsti dalla legge;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- ripartire riserve nei casi in cui ciò non è consentito dalla legge;
- acquistare o sottoscrivere azioni della Società e/o delle sue controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- aumentare fittiziamente il capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti ed informazioni da questi richiesti, ovvero fornendo documenti ed informazioni incompleti, non chiari o fuorvianti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del collegio sindacale o della società di revisione;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- effettuare operazioni straordinarie in violazione delle disposizioni di legge a tutela dei creditori;
- attribuire incarichi di consulenza alla società di revisione o ad altre società dello stesso gruppo, in violazione di norme di legge o dei principi della professione di revisore contabile;
- utilizzare le disponibilità finanziarie per commettere il reato di corruzione;
- intrattenere rapporti e inviare alla controparte informazioni che non siano sempre all'insegna della trasparenza, veritiere, documentate e verificabili;
- erogare servizi fittizi, non necessari, a prezzi non definiti sulla base delle policy aziendali, allo scopo di determinare redditi imponibili non corretti/veritieri o di creare fondi utilizzabili per scopi corruttivi.

4.1.7. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (art. 25 quinquies D.lgs 231/01)

➢ ***Intermediazione illecita e sfruttamento del lavoro (art. 603bis c.p.)***

È punito chiunque:

1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori.

   Costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

   - la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
   - la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
   - la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro.

2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al punto 1, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

SANZIONI

- sanzione pecuniaria: 400 - 1000 quote
- sanzioni interdittive per una durata non inferiore ad un anno.

DIVIETI GENERALI

Con riferimento ai delitti contro la personalità individuale menzionati al paragrafo 4.1.7. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico:

- obbligo di prevedere chiare modalità di controllo atte a regolamentare il monitoraggio in caso di appalto, compresa l'effettuazione di sopralluogo ed altre attività di verifica anche preliminari;
- divieto di subappalto, ovvero, nei casi in cui sia consentito, obbligo per il fornitore di ottenere la previa autorizzazione da parte della Società (in ogni caso vietato il subappalto totale delle attività previste dall'ordine / contratto);
- obbligo, da parte del fornitore, di attestare sotto la propria responsabilità il possesso, da parte del subappaltatore, di idonei requisiti di economico-finanziaria e tecnico-organizzativa, ferma restando la verifica preventiva del fornitore da parte delle funzioni competenti atte ad accertare l'affidabilità dello stesso anche sotto il profilo etico e di onorabilità nonché economico e patrimoniale;
- obbligo per il fornitore, di attestare sotto la propria responsabilità che le retribuzioni sono in linea con quanto previsto dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale o locale, o comunque proporzionato rispetto alla quantità e qualità del lavoro prestato;
- obbligo di rispettare la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
- obbligo di rispettare la normativa in materia di sicurezza e igiene nei luoghi di lavoro nello svolgimento delle attività dei soggetti alle dipendenze o che agiscono per conto della società.

4.1.8. REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (art. 25 septies D.lgs. 231/01)

➢ ***Omicidio colposo (art. 589 c.p.)***

SANZIONI

- sanzione pecuniaria: 250 - 500 quote
- sanzioni interdittive per una durata non < 3 mesi e non > 1 anno

➢ ***Lesioni personali colpose (art. 590 co. 3 c.p.)***

I soggetti che possono rispondere del reato sono tutti i soggetti tenuti ad osservare o far osservare le norme di prevenzione o protezione, vale a dire i datori di lavoro, i dirigenti, i preposti, i soggetti destinatari delle deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro nonché i medesimi lavoratori.

SANZIONI

- sanzione pecuniaria: fino a 250
- sanzioni interdittive per una durata non > 6 mesi

4.1.9. Ricettazione, riciclaggio e impiego di denaro, beni o altre utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies D.lgs.231/01)

➢ ***Ricettazione (art. 648 c.p.)***

Il reato in esame può essere posto in essere da chiunque, al fine di procurare a sé o ad altri un profitto, acquisti, riceva o occulti denaro o cose provenienti da qualsiasi delitto, fuori dei casi di concorso in detto reato presupposto.

➢ ***Riciclaggio (art. 648-bis c.p.) e Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter)***

Il reato in esame potrebbe realizzarsi laddove soggetti apicali, fuori dei casi di concorso nel reato presupposto, compiano operazioni di sostituzione, trasferimento, o altre operazioni, di denaro o beni provenienti da delitto, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

➢ ***Autoriciclaggio (art. 648 ter-1 c.p.)***

E' punito chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa. Il reato in esame si realizza se sussistono contemporaneamente le tre seguenti circostanze:

1) sia creata o si concorra a creare – attraverso un primo reato, il reato presupposto, una provvista consistente in denaro, beni o altre utilità;
2) si impieghi la predetta provvista, attraverso un comportamento ulteriore ed autonomo, in attività imprenditoriali, economiche e finanziarie;
3) si crei un concreto ostacolo alla identificazione della provenienza delittuosa della anzidetta provvista.

Si ritiene che il reato possa principalmente esser posto in essere nell'ambito delle attività connesse alla amministrazione e finanza, ovvero ad opera o con il concorso dei vertici apicali aziendali.

Va sottolineato al riguardo che il D. Lgs. 184/2021 e il D. Lgs. 195/2021 hanno esteso la punibilità dei reati di cui all' art. 25-octies (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio) - in precedenza perseguibili solo se derivanti da condotte di natura dolosa - anche in relazione ai proventi di delitti colposi e contravvenzioni.

SANZIONI

- sanzione pecuniaria: 200 - 800 quote (400 - 1000 quote se denaro proviene da delitto per il quale è stabilita la pena della reclusione > 5 anni)
- sanzioni interdittive per una durata non > 2 anni

DIVIETI GENERALI

Con riferimento ai delitti menzionati al paragrafo 4.1.9. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- trasferire a qualsiasi titolo denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore alla soglia indicata dalla normativa vigente;
- utilizzare denaro contante come mezzo di pagamento al di fuori dei casi consentiti dai principi specifici di cui al presente Modello e dalle procedure aziendali;
- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare quelli eventualmente aperti presso paesi esteri;
- emettere assegni bancari o postali che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare bonifici, anche internazionali, senza indicazione esplicita della controparte;
- disporre pagamenti o incassare denaro verso/da Paesi inseriti nelle principali black list internazionali, senza adeguata documentazione comprovante la reale e specifica necessità;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi, senza adeguata giustificazione contrattuale o comunque non adeguatamente documentati, giustificati e autorizzati;
- affidare lavori, servizi e forniture e disporre i relativi pagamenti senza rispettare i requisiti di forma e tracciabilità richiesti dalle normative vigenti in materia di contratti pubblici e di tracciabilità dei flussi finanziari, ove applicabili;
- tenere un comportamento non corretto e trasparente, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/partner, anche stranieri;
- instaurare rapporti o porre in essere operazioni con soggetti terzi qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione di reati di riciclaggio, ricettazione, reimpiego o autoriciclaggio;
- erogare servizi fittizi, non necessari, a prezzi non definiti sulla base di policy aziendali, allo scopo di determinare redditi imponibili non corretti / veritieri o di creare fondi utilizzabili per scopi corruttivi;
- impiegare i proventi di un delitto non colposo in attività economiche o finanziarie, ovvero impiegare gli stessi con finalità speculative.

4.1.10. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-novies D.lgs. 231/01)

➢ ***Abusiva duplicazione di programmi o predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione per elaboratore (art. 171-bis L. 633/1941)***

Il reato in esame potrebbe realizzarsi laddove la Società, per la realizzazione delle proprie attività, utilizzasse programmi per elaboratore contenuti in supporti non contrassegnati dalla SIAE, ovvero abusivamente duplicasse, distribuisse, vendesse o detenesse a scopo imprenditoriale o concedesse in locazione detti programmi.

➢ ***Riproduzione, trasferimento su altro supporto, distribuzione, presentazione in pubblico del contenuto di una banca dati (art. 171 L. 633/1941)***

Il reato in esame potrebbe realizzarsi laddove la Società, per lo svolgimento delle proprie attività, ovvero anche nell'attività di formazione rivolta ai dipendenti, ovvero nelle attività di comunicazione, utilizzasse, riproducendoli, trasmettendoli o diffondendoli in pubblico, in tutto o in parte, del contenuto di una banca dati

➢ ***Estrazione o reimpiego della banca dati (art. 171-bis L. 633/1941);***

➢ ***Distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis L. 633/1941)***

➢ ***Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies L. 633/1941);***

➢ ***Importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE (art. 171-bis L. 633/1941).***

Si tratta, data la specifica attività di TCS, di ipotesi residuali rispetto a quelle contemplate negli artt. 25 e 25-bis.1 .

SANZIONI

- sanzione pecuniaria: fino a 500
- sanzioni interdittive per una durata non > 1 anno

DIVIETI GENERALI

Con riferimento ai delitti menzionati al paragrafo 4.1.11. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- porre in essere qualsiasi atto dispositivo e/o di utilizzazione, in qualsiasi forma o modalità, di opere artistiche, software, banche dati o opere dell'ingegno di cui la Società non detenga esclusiva proprietà e/o legittimo titolo all'uso;
- duplicare, senza averne titolarità o diritto, ovvero trasmettere a soggetti terzi contenuti che potrebbero essere protetti dal diritto d'autore;
- effettuare download illegali di contenuti multimediali, opere, database o programmi informatici che potrebbero essere coperti da diritto d'autore;

- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o in supero dei diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- duplicare, comunicare a terzi o trasferire su altro supporto il contenuto di una banca dati di terzi, fuori dal legittimo titolo all'uso.

4.1.11. REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA (art. 25 decies D.lgs. 231/01)

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

Il reato in esame si configura laddove si induca taluno, con violenza o minaccia, ovvero mediante promessa di denaro o altra utilità, a non rendere dichiarazioni all'Autorità Giudiziaria ovvero a rendere all'Autorità Giudiziaria dichiarazioni mendaci.

Il reato potrebbe essere commesso in tutte tutte le aree dell'Azienda.

SANZIONI

- sanzione pecuniaria: fino a 500

DIVIETI GENERALI

Con riferimento ai delitti menzionati al paragrafo 4.1.12. e fatto salvo quanto previsto, per ogni area a rischio, nei protocolli specifici, coerentemente con i principi del Codice Etico, è fatto espresso divieto di:

- porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa, nel corso del procedimento penale;
- condizionare o indurre, in qualsiasi forma e con qualsiasi modalità, la volontà dei soggetti chiamati a rispondere all'autorità giudiziaria al fine di non rendere dichiarazioni o dichiarare fatti non rispondenti al vero;
- accettare denaro o altra utilità, anche attraverso terzi esterni alla Società, se coinvolti in procedimenti penali;
- promettere o offrire denaro, omaggi o altra utilità a soggetti coinvolti in procedimenti penali o persone a questi vicini.

I Destinatari dovranno inoltre:

- nei rapporti con l'Autorità giudiziaria, prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti;
- avvertire tempestivamente l'Organismo di Vigilanza di ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente;
- avvertire tempestivamente l'Organismo di Vigilanza di ogni minaccia, pressione, offerta o promessa di danaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da utilizzare in procedimenti penali;
- esprimere liberamente le proprie rappresentazioni dei fatti o esercitare la facoltà di non rispondere, accordata dalla legge, se indagati o imputati in procedimenti penali.

4.1.12. REATI AMBIENTALI (art. 25-undecies D.lgs. 231/01)

➢ ***Inquinamento ambientale (art. 452-bis c.p.) e Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)***

Il reato potrebbe configurarsi laddove la Società cagionasse una compromissione o un deterioramento significativo e misurabile dell'acqua e dell'aria o di porzioni significative del suolo o del sottosuolo nello svolgimento delle proprie attività.

SANZIONI

- sanzione pecuniaria: 250 – 600 quote

4.1.13. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (art. 25 duodecies D.lgs. 231/01)

Il reato potrebbe realizzarsi laddove la Società impiegasse alle proprie dipendenze lavoratori stranieri privi di permesso di soggiorno regolare e/o in corso di validità. A tal riguardo dovrà farsi riferimento anche a lavoratori formalmente non inquadrati come dipendenti della Società, ma che potrebbero rivendicare l'accertamento e/o la costituzione del rapporto di lavoro (ad es. somministrazioni irregolari e altre ipotesi previste dalla legge).

SANZIONI

- sanzione pecuniaria: 100 – 200 quote, entro il limite di 150.000 euro.

4.1.14. REATI TRIBUTARI (Art. 25 quinquiesdecies D.lgs. 231/01)

I reati inseriti nell'art.25-quinquiesdecie in una prima fase dall'art. 39 Decreto Legge n. 124 del 26 ottobre 2019 coordinato con la Legge di conversione n.157 del 19 dicembre 2019 sono stati:

➢ ***Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti Art. 2 D.Lgs. 74:***

Il reato si considera commesso quando l'Ente si avvale di fatture o altri documenti per operazioni inesistenti, sempre che tali fatture o documenti siano registrati nelle scritture contabili obbligatorie o detenuti come prova nei confronti dell'Amministrazione Finanziaria.
Il reato è a consumazione istantanea e si realizza nel momento della presentazione della dichiarazione dei redditi. La mera predisposizione e la registrazione dei documenti attestanti operazioni inesistenti sono condotte meramente preparatorie e non punibili, nemmeno a titolo di tentativo.

- sanzione pecuniaria: fino a 500 quote

➢ ***Dichiarazione fraudolenta mediante altri artifici - Art. 3 D.Lgs. 74***

Il fatto si considera commesso avvalendosi di documenti falsi quando questi sono registrati nelle scritture contabili obbligatorie o detenuti a fini di prova nei confronti dell'Amministrazione Finanziaria.

- sanzione pecuniaria: fino a 500 quote

➢ ***Emissione di fatture o altri documenti per operazioni inesistenti - Art. 8 D.Lgs. 74***

La condotta consiste nell'emettere o rilasciare fatture o altri documenti per operazioni inesistenti e quindi, nella cessione a terzi di documenti fiscali ideologicamente falsi. L'obiettivo è di consentire a terzi

l'evasione sui redditi o sul valore aggiunto, nonché di consentire il conseguimento dell'indebito rimborso o il riconoscimento di un credito d'imposta inesistente.

- sanzione pecuniaria: fino a 400 quote

➢ ***Occultamento o distruzione di documenti contabili - Art. 10 D.Lgs. 74***

Il reato è considerato perfezionato nel momento in cui l'occultamento o la distruzione delle scritture contabili provocano, come effetto diretto, l'impossibilità di ricostruire la situazione reddituale o la ricostruzione del volume d'affari del contribuente.

- sanzione pecuniaria: fino a 400 quote

➢ ***Sottrazione fraudolenta al pagamento di imposte -Art.11 D.Lgs. 74***

Il reato è considerato di "pericolo concreto" poiché richiede che l'atto simulato di alienazione o gli altri atti fraudolenti sui propri o altrui beni siano idonei ad impedire il soddisfacimento totale o parziale del credito tributario da parte dell'Erario. La condotta punita è connotata dallo scopo di rendere inefficace, per sé o altri, la procedura di riscossione coattiva o di ottenere un pagamento inferiore delle somme complessivamente dovute.

- sanzione pecuniaria: fino a 400 quote

Tali reati tributari rilevano ai fini della responsabilità dell'ente ex decreto 231 e, al contempo, possono dare origine anche al delitto di autoriciclaggio.
Mentre quelli inseriti da D.Lgs.n.75 del 14 luglio 2020 sono:

➢ ***Dichiarazione infedele -Art.4 D.Lgs. 74/2000***

- sanzione pecuniaria: fino a 300 quote

➢ ***Omessa dichiarazione -Art.5 D.Lgs. 74/2000***

- sanzione pecuniaria: fino a 400 quote

➢ ***Indebita compensazione - Art.10 quater D.Lgs. 74/2000***

- sanzione pecuniaria: fino a 400 quote

Questi ultimi tre reati tributari rilevano, ai fini della responsabilità amministrativa dell'ente, esclusivamente qualora commessi **nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.**
Sembrano pertanto interessare solo enti di grandi dimensioni e forza economica e solo condotte fraudolenti su scala internazionale.

5. LE AREE A RISCHIO REATO

5.1. ATTIVITÀ COMMERCIALI E DI VENDITA DEI PRODOTTI E SERVIZI

5.1.1. ATTIVITA' A RISCHIO

Le macro-attività individuate dalla Società 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;
- contatto diretto e gestione relazioni con i rappresentanti di Clienti/potenziali Clienti;
- commercializzazione prodotti con loghi e marchi dei "Vendor";
- negoziazione tecnica ed economica dell'Ordine/Contratto; formalizzazione del contratto con i Clienti e/o conferma ed accettazione ordini dei Clienti;
- gestione degli agenti/partner commerciali;
- predisposizione e presentazione della documentazione di offerta per la partecipazione a procedure di selezione della Pubblica Amministrazione (PA) ovvero a trattative con soggetti privati.

5.1.2. 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* (art. 318, 319 c.p.): a titolo esemplificativo e non esaustivo, il prezzo della corruzione potrebbe essere corrisposto sia mediante denaro (a tal fine rilevando la gestione delle risorse finanziarie da parte della Società), sia mediante altre utilità, quale il coinvolgimento in determinati progetti e/o commesse, contratti di fornitura di beni o servizi, assunzione di personale o consulenti di gradimento del soggetto terzo corrotto.
- *Concussione* (art. 317 c.p.) e *Induzione indebita a dare o promettere utilità* (art. 319 quater c.p.): tale forma di reato potrebbe ravvisarsi nell'ipotesi in cui un dipendente della Società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).
  Destinatario della condotta di reato potrebbe essere altresì un soggetto che rivesta contestualmente la qualifica di competitor dell'Ente e di fornitore del medesimo, e in tale ottica, sempre a titolo esemplificativo, tale soggetto potrebbe essere costretto a non concorrere contro l'Ente per l'affidamento di servizi da parte di terzi, pena la perdita degli incarichi quale fornitore di Teleconsys.
- *Corruzione tra privati e Istigazione alla corruzione tra privati* (art. 2635 bis c.c.): il reato in esame potrebbe realizzarsi, a titolo esemplificativo, nei rapporti con clienti o fornitori per acquisire ordini/contratti a condizioni favorevoli.
- *Truffa a danno dello Stato o di un altro ente pubblico o dell'UE* (art. 640 c. 2, n. 1 c.p.): tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta) al fine di ottenere l'aggiudicazione della gara stessa, ovvero si indichino aspetti tecnici non veritieri o referenze non esistenti.

- *Turbata libertà dell'industria o del commercio* (art.513c.p.) *e Illecita concorrenza con minaccia o violenza* (art. 513-bis c.p.)
  il reato potrebbe realizzarsi laddove un soggetto apicale o un dipendente ponesse in essere condotte violente o fraudolente tese a turbare l'esercizio dell'attività imprenditoriale altrui, eventualmente anche per finalità concorrenziali. A titolo esemplificativo, nei confronti di soggetti che rivestano contestualmente la qualifica di concorrenti e di fornitori della Società, ovvero nei confronti di concorrenti che abbiano rapporti con i fornitori della società o con i dipendenti della stessa, sicché nei loro confronti possano realizzarsi le condotte di pressione tipiche della fattispecie.
- *Ricettazione* (art. 648 c.p.)
  a titolo esemplificativo il reato in esame potrebbe realizzarsi 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.
- *Riciclaggio* (art. 648-bis c.p.) e Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter)
  a titolo esemplificativo il reato in esame potrebbe realizzarsi con riferimento a contratti con parti terze, pagamenti e operazioni su conti correnti, ovvero, pur tenendo conto dell'esiguità delle somme, con riferimento all'utilizzo dei contanti ricevuti attraverso rimborsi spese.
- *Autoriciclaggio* (art. 648 ter-1 c.p.)
  il reato in esame potrebbe realizzarsi laddove soggetti apicali o dipendenti, avendo commesso o concorso a commettere un delitto non colposo, compiano operazioni di sostituzione, trasferimento, impiego di denaro o altri beni provenienti da predette attività delittuose, anche colpose, in modo da ostacolarne l'identificazione della loro provenienza delittuosa.
- *Associazione per delinquere* (c.p.416, escluso comma 6)
  tale delitto può realizzarsi in tutti i casi in cui tre o più persone si associno allo scopo di commettere più delitti, tra quelli mappati nel presente Modello, rilevanti ai fini del D.lgs. 231/01, ovvero anche al fine di commettere reati che non siano ricompresi nel catalogo dei reati presupposto dal D.lgs. 231/01.
- *Frode nell'esercizio del commercio* (art. 515 c.p.)
  il delitto si configura laddove, nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico, il venditore consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.
- *Vendita di prodotti industriali con segni mendaci* (art. 517 c.p.)e *Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale* (art. 517-ter c.p.)
  potrebbero 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".

5.1.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività commerciali e di vendita di beni e servizi sono svolte, con riferimento alla fase di definizione ed approvazione delle offerte, conclusione dei contratti e partecipazione alle procedure di evidenza pubblica, nel rispetto:

1. **delle procedure della Società (che definiscono modalità operative, flussi informativi, strumenti e responsabilità), prevedendo, tra l'altro, quanto segue**:

- tutti coloro, all'interno di Teleconsys, che mantengono formali rapporti con la P.A. devono essere

formalmente abilitati mediante apposita delega o disposizione organizzativa (per dipendenti ed organi sociali) oppure mediante specifico contratto (per collaboratori, consulenti o partner);

- le informazioni, dichiarazioni o comunicazioni rese alla P.A. devono contenere solo dati e notizie completi, veritieri, trasparenti ed oggetto preventivo di verifica e supervisione effettuate della funzione gerarchicamente superiore e dalla funzione legale, nonché di tracciabilità e ricostruibilità ex post;
- agli incontri con i Pubblici Ufficiali o gli incaricati di pubblico servizio, in particolare laddove vengano trattate questioni di natura economica o contrattuale, devono preferibilmente partecipare almeno due responsabili Teleconsys;
- non devono essere tenuti comportamenti con pubblici ufficiali o incaricati di pubblico servizio volti ad ottenere indebiti vantaggi a favore dell'ente;
- in caso di procedure di evidenza pubblica, i responsabili delle relative funzioni stabiliscono tempistiche per la preparazione e caricamento della documentazione;
- sono previsti 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;
- sono monitorati e costantemente aggiornati i requisiti ex art. 80 d.lgs. 50/2016 e s.m.i. per partecipazione a gare (certificazioni, adempimenti fiscali, previdenziali, DURC, DURF, ecc..);
- prima di avviare relazioni commerciali con un nuovo cliente, è svolta una preliminare verifica della presenza sulla controparte di adeguati requisiti finanziari, etici, morali e reputazionali per evidenziare elementi di criticità o di rischio;
- il responsabile di area, laddove necessario e rilevante, comunica all'ODV i nominativi dei soggetti con i quali Teleconys ha avviato relazioni commerciali nonostante siano stati evidenziati elementi di criticità o di rischio dall'analisi delle informazioni preliminari ricevute;
- le informazioni di ciascuna vendita sono confinate a ciascun Account assegnato, il sistema informativo che gestisce le informazioni commerciali è profilato in accordo al "business need";
- la selezione dei distributori ("vendor") per l'acquisto di prodotti e servizi è effettuata realizzando il miglior compromesso di scelta tra vantaggio economico e tecnico;
- con le Società produttrici di beni HW e SW sono stipulati Accordi di partnership che definiscono nel dettaglio le condizioni di rivendita dei prodotti;
- prima di essere trasmessa al Committente, l'offerta tecnica e l'offerta economica sono esaminate col coinvolgimento di più Funzioni della Società, in base ai rispettivi ambiti di competenza, in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- l'offerta è accompagnata dalle condizioni generali di vendita (specifiche di fornitura, termini e modalità di pagamento, ecc) che devono essere sottoscritte per accettazione dal Cliente insieme alla informativa sul trattamento dei dati personali;
- i contratti sottoscritti dalla Società sono, di norma, elaborati sulla base di formati standard, e sono sottoposti alle Funzioni della Società in base ai rispettivi ambiti di competenza, per valutazione e condivisione;
- i contratti devono prevedere la presenza di specifiche clausole contrattuali a tutela e corretto utilizzo dei diritti di proprietà intellettuale, marchi e brevetti;
- i contratti devono prevedere uno specifico rimando alle regole di condotta contenute nel Codice Etico e Modello ex D.Lgs. 231/01, avuto riguardo a correttezza, trasparenza e leale collaborazione, la cui violazione determina la risoluzione del contratto stesso;
- 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;
- ciascun contratto stipulato con il cliente prevede la firma autorizzativa del Rappresentante Legale dell'azienda o di altro rappresentante che ne abbia procura, previo controllo dei poteri di firma;
- anche lato Cliente vanno verificati i poteri di rappresentanza e di firma;
- per ogni contratto attivo stipulato devono, di norma, essere redatti specifici contratti passivi con il fornitore, in maniera sostanzialmente speculare, definendo analoghi livelli di dettaglio dei contenuti, dei prezzi e dei livelli di servizio;
- i contratti e tutta la documentazione relativa alla trattativa commerciale ed alle valutazioni effettuate sul Cliente sono conservati nel rispetto delle modalità e dei termini di legge.

2. **dei principi espressi nel Codice Etico. In particolare, è esplicitamente vietato**:

- offrire o eseguire, direttamente o indirettamente, pagamenti indebiti e promesse di vantaggi personali, di qualsiasi natura, ai rappresentanti della Pubblica Amministrazione;
- elargire omaggi o regali, liberalità o donazioni finalizzati all'acquisizione impropria di benefici in favore di funzionari pubblici, loro familiari e persone con le quali i funzionari intrattengono notoriamente stretti legami;
- utilizzare, nella gestione dei rapporti con la Pubblica Amministrazione, eventuali percorsi preferenziali o conoscenze personali, al fine di influenzarne indebitamente le decisioni;
- ricorrere a forme di pressione, inganno tali da influenzare le conclusioni dell'attività amministrativa.

5.2. GESTIONE DEGLI ACQUISTI DI BENI E SERVIZI DA TERZI

5.2.1. ATTIVITÀ A RISCHIO

Le macro-attività individuate dalla Società come a potenziale rischio nell'ambito della presente area 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;
- analisi comparata delle quotazioni e procedure di selezione del fornitore;
- gestione della qualifica/certificazioni dei beni acquistati (ove richiesto);
- negoziazione dei prezzi e definizione degli accordi contrattuali;
- emissione dell'Ordine di Acquisto o del contratto e dei connessi adempimenti;
- incarichi di consulenza o prestazione professionale assegnati alle persone fisiche:
- 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

5.2.2. 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:

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

  Tale forma di reato potrebbe ravvisarsi nell'ipotesi in cui un dipendente della Società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute nell'ambito delle attività di acquisti di beni e servizi o negli incarichi connessi alla manutenzione della sede (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).
- *Corruzione per l'esercizio della funzione e/o corruzione per un atto contrario ai doveri d'ufficio* (art. 318, 319 c.p.)

  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.
- *Corruzione ed istigazione alla corruzione tra privati* (art. 2635 bis c.c.)

  tale forma di reato potrebbe configurarsi nell'ipotesi in cui, ad esempio, un referente della Società dia, offra o prometta denaro o altra utilità al fornitore per ottenere un indebito beneficio, quale uno sconto fuori mercato o anticipazione delle consegne.

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

  l'ipotesi di reato si potrebbe ricondurre all'alterazione di registri informatici della Pubblica Amministrazione per far risultare esistenti condizioni essenziali per la partecipazione a gare (iscrizione in albi, ecc.), ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti.
- *Associazione per delinquere* (art. 416, escluso comma 6 c.p.)

  l'ipotesi di reato si potrebbe configurare laddove si stabilisca un patto associativo tra Società e fornitori, per alterare i risultati delle gare al fine di spartire i benefici economici derivanti da tale comportamento, attraverso, ad esempio, l'ottenimento di un significativo risparmio economico sulle forniture.
- *Ricettazione* (art. 648 c.p.)

  nell'ipotesi di acquisto di beni provenienti da un qualsiasi delitto, anche colposo, 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).
- *Riciclaggio* (art. 648-bis c.p.) e Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter)

  il reato potrebbe configurarsi in astratto nel caso in cui la Società si accordi con il fornitore per eludere le regole in tema di tracciabilità dei flussi finanziari.
- *Autoriciclaggio* (art. 648 ter-1 c.p.)

  nel caso in cui, a seguito della commissione o del concorso in commissione di un delitto 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.
- *Reati contro la personalità individuale* (art. 25-quinquies D.lgs 231/01): Il reato di Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.) e di Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 12 D.Lgs. 286/1998)

  potrebbero in astratto configurarsi in concorso con i fornitori/appaltatori, per attività da questi svolte sotto il controllo di Teleconsys, consentendo dei risparmi economici anche nell'acquisto di servizi (ad es. somministrazioni irregolari e altre ipotesi previste dalla legge).

5.2.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto di quanto già indicato nel Codice Etico, delle procedure aziendali e dei seguenti principi cardine:

Richiesta di acquisto

- occorre garantire un'adeguata separazione dei compiti nel processo di acquisizione di beni e servizi (Separation of duties);
- la richiesta di acquisto deve essere formalizzata e autorizzata seguendo lo specifico iter, laddove rientri nell'ambito del budget approvato.

Selezione e scelta delle offerte di fornitura

- sono previste specifiche regole di condotta verso i fornitori nel Codice Etico, relative a correttezza, trasparenza, imparzialità nelle scelte e non discriminazione, pari opportunità. In particolare:
    - la scelta dei fornitori deve essere eseguita sulla base di criteri imparziali, oggettivi e documentabili;
    - sono espressamente vietati acquisti effettuati verso fornitori scelti principalmente in base a criteri di amicizia, parentela o qualsiasi altra cointeressenza tale da inficiarne la validità in termini di prezzo e/o qualità o che risultino strumentali alla realizzazione di una delle condotte illecite indicate nel Decreto;
    - è vietato indurre un fornitore a stipulare un contratto a lui sfavorevole lasciandogli intendere un successivo contratto più vantaggioso;
    - è vietato negoziare condizioni contrattuali occulte che non risultino da idonea documentazione conservata unitamente alla documentazione relativa all'acquisto.
- preliminarmente all'avvio del rapporto contrattuale è effettuata un'adeguata verifica sulle controparti (visura camerale, solidità finanziaria, sede legale/amministrativa non in Paesi Black List, ottenimento autodichiarazione ai sensi degli artt. 88 e 89 del D.lgs. 159/2011);
- è richiesta una pluralità di preventivi, la cui valutazione va effettuata in un'ottica volta ad assicurare la migliore configurazione possibile di costo, qualità e tempo per la Società. Acquisti "vincolati" ad un unico fornitore vanno motivati in forma scritta;
- i Fornitori che intrattengono rapporti con Teleconsys sono tenuti a conformarsi a specifiche regole di condotta, cui aderiscono mediante sottoscrizione del Codice di condotta Fornitori.

Sottoscrizione dell'ordine/contratto

- sono preliminarmente stabilite le condizioni economiche e tecniche coerenti con la tipologia di fornitura richiesta;
- salvo stipulazione di contratti specifici, i Fornitori sottoscrivono per accettazione le Condizioni generali di acquisto di beni e servizi di Teleconsys, che contengono le norme idonee a tutelare l'interesse sociale (verifica di conformità, penali, responsabilità del fornitore, proprietà intellettuale, rispetto del Modello 231/01, obblighi di riservatezza, Trattamento dei dati personali, ecc.);
- in caso di forniture relative a commesse, è verificata la congruenza tra modalità di fornitura/termini di pagamento del Cliente e condizioni pattuite col fornitore;
- gli Ordini/Contratti sono sottoscritti dal soggetto della Società dotato di idonea procura in tal senso;
- anche lato fornitore vanno verificati i poteri di rappresentanza e di firma.

Ricezione, controllo e valutazione della fornitura e di autorizzazione al pagamento

- Verifica dell'avvenuta ricezione dell'approvvigionato secondo quanto previsto da ordine a fornitore e sollecito in caso di mancata consegna rispetto ai termini contrattualmente stabiliti;
- eventuali criticità/inadempimenti o parziali adempimenti di obbligazioni contrattuali sono contestati per iscritto e gestiti dalle Funzioni aziendali competenti, in coordinamento con la Funzione legale;
- la Funzione aziendale competente attesta l'effettività della prestazione, previa acquisizione della relativa documentazione, prima della liquidazione del relativo corrispettivo;
- separazione funzioni tra soggetto che riceve la fornitura e chi contabilizza la fattura del fornitore e ne effettua il pagamento;
- valutazione del fornitore avvalendosi del "*Qualification Form*", che valuta i seguenti KPI, ai fini dell'assegnazione del Rating: Qualità del Servizio; Tempi di consegna; Supporto Tecnico / Prep. Personale; Prezzi rispetto al mercato; Tempi di pagamento.

Archiviazione dei dati/documenti/atti predisposti nel corso delle attività (richieste di offerta, motivazione della scelta, DDT, ecc.), per assicurare la tracciabilità del processo di gestione degli acquisti di beni e servizi e per poter gestire eventuali contenziosi.

Incarichi di consulenza o prestazione professionale assegnati alle persone fisiche

è richiesto e attentamente valutato il possesso da parte del consulente di requisiti soggettivi di esperienza, affidabilità e competenza professionale per l'espletamento dell'incarico;

- i contratti sono redatti secondo un formulario standard che assicura omogeneità di forma e contenuto;
- i contratti contengono le clausole idonee a tutelare l'interesse sociale (responsabilità del consulente, autonomia organizzativa, proprietà intellettuale, rispetto del Modello 231/01, obblighi di riservatezza, Trattamento dei dati personali, ecc..);
- sono formalmente individuati i rappresentanti della Società delegati a negoziare, stipulare e controllare detti contratti;
- sono formalmente individuati i rappresentanti della Società delegati ad effettuare attività di
- supervisione e monitoraggio costante delle attività svolte dal professionista.

5.3. REALIZZAZIONE COMMESSE, "DELIVERY" E SERVIZI

5.3.1. ATTIVITÀ A RISCHIO

Le macro-attività individuate come a potenziale rischio nella presente area, possono essere riepilogate come segue:

- raccolta delle esigenze per esecuzione commessa;
- pianificazione delle attività e delle scadenze (aspetti tecnici, economici e tempistiche);
- verifiche e adempimenti amministrativi propedeutici all'avvio delle attività (contratti, garanzie, autorizzazioni, ecc.);
- definizione degli SLA (Service Level Agreement);
- interfaccia continuativa con il cliente e con il fornitore agli adeguati livelli;
- verifica e approvazione della documentazione di progetto;

- gestione e verifica formale degli avanzamenti periodici in occasione dei SAL;
- monitoraggio e rispetto SLA per servizi ICT;
- verifica e approvazione della rendicontazione;
- verifiche di conformità/collaudi e autorizzazione all'emissione delle fatture da parte del Committente;
- controllo dell'andamento economico/finanziario;
- attivazione delle licenze;
- verifica presupposti ed autorizzazione atti modificativi ed integrativi dei contratti (proroghe, varianti, sospensioni ecc.);
- gestione delle eventuali criticità di natura tecnica e delle contestazioni (sia nei confronti dei fornitori sia nei confronti dei clienti);
- 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;
- conservazione documentazione relativa diverse fasi commessa (DDT, rapportini, originali contratti, ecc).

5.3.2. 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 seguenti reati:

- *Ricettazione* (art. 648 c.p.)
  nell'ipotesi di utilizzo, nelle diverse fasi di delivery, di risorse di provenienza illecita.
- *Autoriciclaggio* (art. 648 ter-1 c.p.)
  nel caso in cui, a seguito della commissione o del concorso in commissione di un delitto tra quelli previsti nell'area a rischio in oggetto, si ottengano delle utilità che sono impiegate, nelle diverse fasi di delivery, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
- *Corruzione tra privati ed istigazione alla corruzione tra privati* (art. 2635 bis c.c.)
  nell'ipotesi in cui un referente delle Società corrompa o tenti di corrompere, anche per interposta persona, il Cliente privato al fine di evitare che siano evidenziate delle problematiche riscontrate nello svolgimento delle attività di delivery (difetti, malfunzionamenti, o non conformità dei prodotti consegnati).
- *Corruzione per l'esercizio della funzione e/o corruzione per un atto contrario ai doveri d'ufficio* (art. 318, 319 c.p.)
  nell'ipotesi in cui un referente delle Società corrompa o tenti di corrompere, anche per interposta persona, i rappresentati della PA ad accettare, in cambio di utilità, forniture non conformi, o ad omettere di comminare le penali ovvero ad approvare varianti tecniche ed economiche non giustificate dalle effettive esigenze.
- *Concussione* (art. 317 c.p.) e *Induzione indebita a dare o promettere utilità* (art. 319 quater c.p.)
  nell'ipotesi in cui un dipendente della Società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute, ad esempio, nell'ambito delle attività di collaudo e di verifica di buona esecuzione e approvazione dei SAL (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).
- *Indebita percezione di erogazioni a danno dello Stato* (art. 316-ter c.p.)
  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.

- *Truffa e truffa aggravata per il conseguimento di erogazioni pubbliche* (art. 640 c. 2, n. 1 c.p.)
  la linea di demarcazione con la fattispecie precedente risiede nel tipo di condotta criminosa del reo che, nel primo caso, si limita a presentare documenti falsi o ad omettere informazioni dovute; mentre in questa seconda ipotesi pone in essere artifizi o raggiri che provocano l'induzione in errore della Pubblica Amministrazione.
- *Frode nelle pubbliche forniture* (art. 356 c.p.)
  il reato in esame potrebbe verificarsi ad esempio, in caso di consegna - mediante espediente malizioso o inganno - di un prodotto o servizio diverso da quello pattuito nell'esecuzione di un contratto, nell'ambito di pubbliche forniture.
- *Reati di omicidio colposo, art. 589 c.p. e lesioni colpose gravi o gravissime, art. 590 co. 3 c.p., commessi con violazione delle norme antinfortunistiche sulla tutela della salute e sicurezza sul lavoro* (art. 25-septies D.lgs. 231/01)
  i soggetti che possono rispondere del reato sono tutti i soggetti tenuti ad osservare o far osservare le norme di prevenzione o protezione, vale a dire i datori di lavoro, i dirigenti, i preposti, i soggetti destinatari delle deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro nonché i medesimi lavoratori.
  Il delitto in esame potrebbe realizzarsi in caso di decesso di un lavoratore nello svolgimento di una commessa, in conseguenza di una violazione delle norme per la prevenzione degli infortuni sul lavoro e/o della inidoneità delle misure di prevenzione adottate.
- *Reati contro la personalità individuale* (art. 25-quinquies D.lgs 231/01)
  Il reato di Intermediazione illecita e sfruttamento del lavoro (art. 603bis) e il reato di Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies D.lgs. 231/01) per l'attività svolta da Teleconsys con lavoratori sotto il suo diretto controllo.
- *Frodi contro le industrie nazionali* (art. 514 c.p.)
  nell'ipotesi in cui nello svolgimento delle attività di commessa si forniscano prodotti con nomi, marchi o segni distintivi contraffatti o alterati, anche se non registrati.
- *Frode nell'esercizio del commercio* (art. 515 c.p.)
  il carattere plurioffensivo della frode in commercio sussiste anche quando la cosa richiesta dal Cliente non sia tutelata da un marchio o da altra speciale protezione, giacché la norma tutela oggettivamente il leale esercizio del commercio e, quindi, sia l'interesse del cliente a non ricevere una cosa diversa da quella richiesta, sia l'interesse del produttore a non vedere i suoi prodotti scambiati surrettiziamente con prodotti diversi.
- *Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni* (art. 473 c.p.)
  nell'ipotesi in cui nello svolgimento delle attività di commessa si commettano i reati in questione.

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, adotta le seguenti procedure e regole di condotta:

- Redazione "*Piano di delivery*" che contiene la descrizione della fornitura (di beni e/o servizi), il crono programma, le verifiche e adempimenti amministrativi propedeutici all'avvio delle attività, dettagli sull'esecuzione, SLA e obiettivi di miglioramento;

- individuazione di un team di risorse coordinate dal *Project Manager* o "*Delivery Leader*" (PM/DL) a seconda della natura dell'attività contrattuale, dedicato all'esecuzione del contratto, con i seguenti compiti:
  - 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 eventuali partner in RTI;
  - verificare i requisiti contrattuali;
  - verificare la corretta rendicontazione dell'impegno da parte delle risorse interne (al fine dell'attribuzione dei costi interni alla commessa);
  - monitorare i contratti di sub-fornitura di beni e servizi riferibili alla commessa, verificando le relative prestazioni;
  - gestire i rapporti con eventuali partner in RTI monitorando anche tutti gli aspetti relativi all'utilizzo condiviso di opere dell'ingegno e segni distintivi;
  - controllare pianificazione e avanzamento lavori, la documentazione di progetto, la verifica qualitativa e funzionale dei prodotti da consegnare (software, infrastruttura, ecc..), il controllo delle quantità pianificate e rendicontate (fatte salve le verifiche previste in fase di verifica di conformità finale), la corretta attivazione delle licenze;
  - richiedere al Cliente, a seguito di verifica/collaudo positivo, l'autorizzazione all'emissione delle fatture in base a scadenzario contrattuale.
- è garantito un adeguato flusso informativo tra il PM/DL e le altre funzioni aziendali coinvolte (es. Ufficio acquisti, Legal, CFO, ecc.) in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- nell'esercizio dei rapporti contrattuali, sono consegnati ovvero utilizzati esclusivamente i beni dichiarati o pattuiti con il Cliente (per origine, provenienza, qualità o quantità);
- la tutela dei diritti di proprietà industriale ed il coordinamento nella loro gestione è svolta durante lo svolgimento di ogni commessa. In particolare:
  - sono svolte apposite verifiche per accertarsi che il SW sviluppato internamente non sia già stato oggetto di brevetto o copyright da parte di terzi;
  - laddove la realizzazione di prodotti e/o esecuzione di servizi comporti l'utilizzo di componenti/prodotti brevettati da terzi, occorre verificare che sia stata rilasciata autorizzazione formale nell'ambito del contratto;
- sono pianificate ed eseguite le attività di collaudo, ovvero le attività di verifica tecnica, dei prodotti/servizi oggetto del contratto da parte delle strutture aziendali preposte, in contraddittorio con il Cliente. Sono redatti e conservati i verbali di SAL o di collaudo parziale ed accettazione da parte del cliente;
- il PM/DL alle scadenze previste procede all'emissione dei SAL ed alla richiesta di emissione fattura attiva all'Area AFC;
- il PM/DL deve verificare l'andamento economico della commessa rispetto a quanto previsto contrattualmente ed a budget in termini di ricavi e costi, sia maturati (consuntivi) che previsti (pianificati), in collaborazione con l'Area AFC, nonché il rispetto dei tempi di fatturazione e di incasso;
- nel caso di mancato rispetto del budget o delle previsioni contrattuali su fatturazioni/incassi, il PM deve evidenziare la criticità e proporre azioni correttive;
- in caso di appalto a terzi di parte della commessa, il PM/DL verifica la corretta esecuzione degli adempimenti in materia di subappalto e subfornitura e la loro conformità agli obblighi contrattuali;
- eventuali criticità di natura tecnica o contestazioni per inadempimenti o parziali adempimenti di

obbligazioni contrattuali sono gestiti dalle Funzioni aziendali competenti, in coordinamento con la Funzione legale;

- ciascuna funzione responsabile di un processo deve garantire la corretta archiviazione e conservazione della documentazione di competenza, sia cartacea che elettronica, nel rispetto della riservatezza, della sicurezza e della normativa vigente (in termini di conservazione dei documenti);
- al termine dell'attività, e al fine di documentarne formalmente la conclusione, i" deliverables" sono sottoposti a verifica di conformità/collaudo finale, viene formalmente registrata con adeguate evidenze documentali.

5.4. SISTEMI INFORMATIVI AZIENDALI

5.4.1. ATTIVITÀ A RISCHIO

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

- definizione Politica di sicurezza e procedure per la protezione dei dati personali e in materia di sicurezza del sistema informatico e telematico proprio e dei clienti;
- gestione e protezione della postazione di lavoro (apparati, sistemi, dispositivi mobili);
- utilizzo internet e posta elettronica da parte dei dipendenti;
- gestione e controllo 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;

gestione e protezione della Rete e delle Infrastrutture di comunicazione Elettronica;

- gestione e protezione di server e database;
- generazione e monitoraggio di log di sistema e applicazioni;
- procedure di backup;
- gestione degli incidenti sulla sicurezza dei sistemi e delle informazioni;
- gestione della sicurezza fisica e ambientale e asset management;
- acquisizione e gestione di apparecchiature, di dispositivi connessi con il sistema o di programmi informatici; erogazione di servizi professionali di installazione, manutenzione e supporto;
- svolgimento attività di Amministratore di sistema presso la Società e presso sistemi di terzi;
- attività di trattamento dei dati personali;
- Smaltimento di supporti e cancellazione dati

5.4.2. 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 dalla Società, quali quelli previsti dall'art. 24-bis (delitti informatici e trattamento illecito di dati) di seguito indicati:

- *Falsità in documenti informatici (art. 491-bis c.p.)*

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

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

  il delitto potrebbe essere commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un partner commerciale, di una stazione appaltante o di un competitor.

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

  il reato in parola potrebbe realizzarsi laddove gli apicali ovvero i dipendenti forniscano a terzi non autorizzati credenziali di accesso a sistemi informatici gestiti da Teleconsys, ovvero consentano a terzi di continuare ad utilizzare le predette credenziali pur non avendone più titolo, al fine di procurarsi un profitto eventualmente derivante dalla relazione con i terzi.

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

  il delitto potrebbe configurarsi, ad esempio, nel caso in cui un dipendente introduca un virus, idoneo ad interrompere il funzionamento di un sistema informatico o telematico di un terzo (concorrente, fornitore o stazione appaltante), o a danneggiare i dati in esso contenuti, o qualora si producano o si utilizzino delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi elettronici.

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

  il reato si perfeziona, ad esempio, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente, con il vantaggio concreto dell'ente di appartenenza.

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

  la fattispecie di reato in questione si considera integrata, con vantaggio dell'ente, nel caso in cui, ad esempio, un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato, si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

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

  il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei dati o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

- *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)*

  questo delitto si distingue da quello di cui al precedente punto poiché in questo caso il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità.

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

  il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuato danneggiando direttamente il sistema, per esempio, attraverso l'inserimento di un virus.

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

  la condotta del dipendente addetto al sistema informatico di un cliente - sistema che deve perseguire uno scopo di pubblica utilità - che, in sede di esecuzione di un contratto di appalto con la Pubblica Amministrazione o con persone incaricate di pubblico servizio, danneggi una parte del sistema medesimo al fine di occultare un inadempimento contrattuale della società dalla quale dipende.

  Tali condotte sarebbero aggravate laddove realizzate su sistemi informatici sui quali la Società o gli addetti della Società rivestano la qualifica di "amministratori di sistema".

- *Frode informatica (art. 640-ter c.p.)*

  Si evidenzia, inoltre, che il "Ransomware" è un tipo di malware che, con la trasmissione di un'e-mail e l'apertura di essa (di un allegato, o cliccando su un link o banner), infetta il sistema informatico e i dati da esso custoditi recapitando la richiesta di riscatto (da pagare in Bitcoin, o altra moneta virtuale) per rimuovere la limitazione. Nel corso della vicenda info-estorsiva, e per la soluzione di essa, con l'eventuale pagamento agli estorsori, si viene a configurare un reato presupposto 231 commesso da esponenti aziendali nell'interesse/vantaggio dell'ente aggredito.

5.4.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La sicurezza delle informazioni e dei sistemi informativi aziendali è assicurata da misure atte a scongiurare, nello specifico, l'applicazione delle sanzioni contenute nell'art. 24- bis del D.lgs. 231/01, sui delitti informatici e trattamento illecito di dati, nell'art. 25-quinquies, sui delitti contro la personalità individuale e nell'art. 25-novies, sui delitti in materia di violazione del diritto d'autore.
La Società promuove l'implementazione ed il mantenimento di un sistema per la gestione della sicurezza delle informazioni conforme alla norma ISO 27001, con la collaborazione di tutte le strutture aziendali coinvolte. In particolare:

- **Politica di sicurezza e procedure per la protezione dei dati personali:**

La Società documenta la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni, approvata dalle figure competenti e comunicata a tutti i dipendenti (in particolare agli incaricati del trattamento) e alle parti esterne interessate.
La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.

- **Ruoli e responsabilità della sicurezza delle informazioni**

I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità alle politiche di sicurezza, inclusa la nomina di un responsabile della sicurezza (Chief Information Security Officer – CISO).
In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, la Società dispone di una procedura definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e per la conseguente riconsegna di dispotici e altri mezzi del trattamento.

- **Politica di controllo degli accessi**

I diritti in merito al controllo degli accessi, i diritti di accesso e le restrizioni sono assegnati a ciascun ruolo in base ai principi di pertinenza e necessità. La segregazione dei ruoli è definita in modo chiaro e

documentato.

- **Gestione risorse/asset**

La Società ha predisposto un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete), che include le seguenti informazioni: risorsa IT, tipo e posizione (fisica o elettronica). Il censimento delle risorse e degli apparati IT e il relativo registro sono rivisti e aggiornati con cadenza periodica e regolare.
La Società si assicura che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da un soggetto specifico

- **Gestione degli incidenti (data breaches)**

È definito un piano di risposta agli incidenti (Incident Response Plan) che prevede procedure dettagliate per garantire una risposta efficace al verificarsi di incidenti o violazioni di dati personali (elenco di possibili azioni di mitigazione; chiara assegnazione dei ruoli).
Le violazioni dei dati personali sono segnalate immediatamente ai soggetti competenti secondo l'organigramma interno. Sono regolate le procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.

- **Business continuity**

La Società ha definito le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT in caso di violazione di dati personali.
E' predisposto e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza), con l'indicazione di i) azioni chiare, ii) assegnazione di ruoli, iii) struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

- **Obblighi di confidenzialità imposti al personale**

La Società richiede, previa sottoscrizione di specifico accordo di riservatezza, che tutti i dipendenti si obblighino a mantenere strettamente riservate e a non rivelare o divulgare a terzi, le informazioni e/o documenti che devono rimanere segreti.

- **Amministratore di Sistema**

La funzione di Amministratore di Sistema è conferita formalmente, 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.

- **Awareness**

La Società garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali sono, inoltre, adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso programmi di formazione strutturati e regolari per il personale.

- **Controllo degli accessi e autenticazione**

L'accesso degli utenti ai sistemi informatici interni è consentito ai lavoratori dipendenti, distaccati e ad utenti esterni preventivamente autorizzati, quale supporto al lavoro giornaliero.
L'assegnazione utenza e profilo di accesso prevede un codice identificativo ("User-id" o "ID") che, utilizzato in abbinamento a una password personale, consente di accedere al sistema. La password deve essere composta da una combinazione di numeri e lettere onde consentire un maggior livello di tutela.
Dopo la prima creazione, la password è a gestione esclusiva dell'utente, che è obbligato a modificarla periodicamente. E' strettamente personale, deve restare segreta e non deve essere comunicata né ai colleghi né a terzi. Il responsabile IT ha comunque sempre la possibilità di forzare il sistema (ad es. in caso di dimenticanza della password da parte di un utente, il responsabile IT crea una nuova password

"temporanea"). Le password di accesso ai sistemi informativi hanno una durata massima definita; raggiunto tale termine esse scadono e devono essere rinnovate dagli utenti.
Per ogni ambiente applicativo l'ID è unico, utilizzabile solo da una persona e non riutilizzabile per altri; viene disattivato definitivamente alla comunicazione della cessazione del rapporto di lavoro. Nei casi di dimissioni/cessazione di dipendenti/distaccati, di interruzione dei contratti con collaboratori o di cessazione del ruolo dei soggetti terzi cui è stato concesso l'accesso ai sistemi, le credenziali di accesso sono disabilitate con immediatezza; nel caso di variazioni di ruolo dei soggetti precedentemente elencati, le abilitazioni delle credenziali di accesso concesse cono modificate con immediatezza per adeguarle al nuovo ruolo.

- **Generazione di file di log e monitoraggio**

Sono generati file di log per ogni sistema/applicazione utilizzata per il trattamento dei dati personali (visualizzazione, modifica, cancellazione).
Sono registrati gli accessi mediante autenticazione informatica ai sistemi informatici e agli archivi elettronici da parte di tutti i dipendenti ivi inclusi gli Amministratori di sistema e le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta/cancellazione/modifica dei diritti dell'utente.
I file di log sono contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Un sistema di monitoraggio genera i file log e produrre report sullo stato del sistema e notificare potenziali allarmi.

- **Sicurezza di Server e Database**

I server, ove risiedono database e applicazioni, sono configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo al fine di garantirne il corretto funzionamento. I suddetti server trattano solo i dati personali effettivamente necessari per il perseguimento delle finalità perseguite.
Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.
Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti al fine di evitare il collegamento con l'interessato in assenza di ulteriori informazioni.

- **Sicurezza delle Postazioni di lavoro**

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al personale sono strumenti di lavoro, pertanto:

- possono essere utilizzati solo per fini lavorativi e non anche per scopi personali;
- vanno utilizzati in modo appropriato;
- devono essere prontamente segnalati alla figura incaricata a ricevere segnalazioni il furto, il danneggiamento o lo smarrimento di tali strumenti;
- non è consentita l'installazione autonoma, nemmeno sul pc in dotazione, di mezzi di proprietà dell'assegnatario (es. modem, stampanti, altre periferiche, software) onde evitare il pericolo dell'introduzione di virus informatici, nonché alterare la stabilità delle applicazioni del computer;
- non è permesso modificare o alterare le configurazioni del pc (in particolare le impostazioni di sicurezza;
- al termine dell'uso del computer occorre sempre chiudere i programmi secondo le appropriate procedure di sicurezza;
- è tassativamente vietata la detenzione di materiale non in regola con la normativa sul diritto di autore (SIAE) e pedo-pornografico, anche virtuale, in quanto costituente reato.

Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base giornaliera. Gli

aggiornamenti critici sulla sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.

- **Sicurezza della Rete e della Posta Elettronica**

Le unità di rete sono aree di condivisione di informazioni strettamente aziendali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato in tali unità. Colui che dovesse creare in rete le cosiddette "cartelle condivise" deve aver cura di concederne l'accesso solo a chi debba esserne coinvolto per motivi di servizio.
Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione avviene in forma crittografata tramite protocolli crittografici (TLS / SSL).
Il traffico di dati da e verso il sistema IT è monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
La Società può, così come raccomandato dal garante della Privacy:

- stilare una "black list" di siti web negativi, anche ai fini della protezione della sicurezza dei sistemi dagli attacchi esterni, bloccandone preliminarmente l'accesso;
- adottare misure come la configurazione di filtri che prevengono l'accesso ai suddetti portali web.

Occorre evitare di navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, sindacali, religiose o di genere del dipendente o del collaboratore in quanto il sistema effettua automaticamente la registrazione degli accessi e, quindi, è potenzialmente idoneo a rivelare dati sensibili concernenti tali soggetti.
E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
E' vietato scaricare software, soprattutto se gratuiti (freeware e shareware), da siti Internet. È altresì proibito copiare e/o utilizzare software in violazione della legge sui diritti d'autore, delle licenze e delle altre tutele giuridiche applicabili.
La posta elettronica è da considerare uno strumento di lavoro e, come tale, soggiace alle seguenti regole:

- l'uso della e-mail deve sempre essere rispettoso delle norme di legge (es.: segreto commerciale, diritto d'autore, riservatezza, privacy ecc.);
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria in relazione a genere, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica anche in ottemperanza ai contenuti dell'art. 25-terdecies D.lgs. 231/01 "Razzismo e xenofobia";
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere potenzialmente intercettata da estranei e, dunque, non deve essere preferibilmente utilizzata per inviare documenti di lavoro aventi natura estremamente riservata;
- l'uso personale della posta elettronica è consentito a patto che esso non interferisca con l'attività lavorativa, non si configuri come un irragionevole dispendio di risorse e non pregiudichi le attività aziendali;
- occorre prestare attenzione ai messaggi di posta elettronica che provengono da persone o enti sconosciuti. non bisogna aprire gli allegati in quanto potrebbero contenere virus (l'estensione degli allegati "infetti" è spesso .PST, LPS, .EXE.).

L'utilizzo delle PEC aziendali è limitato ai soli dipendenti all'uopo espressamente autorizzati.

- **Back-up**

Le procedure di backup e ripristino dei dati sono definite, documentate e collegate a ruoli e responsabilità.
Le copie del backup sono conservate in modo sicuro in luoghi diversi.
I backup incrementali programmati sono eseguiti almeno su base giornaliera.
Laddove siano utilizzati servizi per l'archiviazione di backup resi da fornitori esterni, la copia prima di essere trasmessa viene crittografata.

- **Privacy**

La Direzione provvede, in collaborazione con il DPO, a definire la periodicità con cui deve essere eseguita la formazione in materia privacy e sicurezza delle informazioni ed a pianificarla in accordo a tale periodicità d'intesa con l'ufficio del personale.
I fornitori/consulenti/collaboratori devono sottoscrivere appositi impegni nel caso trattino dati personali di cui Teleconsys e/o i Committenti siano Titolari.
Nei contratti/ordini che Teleconsys stipula con fornitori, consulenti, e collaboratori vengono inseriti i requisiti per la gestione della sicurezza delle informazioni.
E' redatto e costantemente aggiornato il registro dei trattamenti effettuati dalla Società sia in qualità di Titolare (cd. trattamenti interni) che di Responsabile (cd. trattamenti esterni).

5.5. SELEZIONE, GESTIONE, FORMAZIONI ED AMMINISTRAZIONE DEL PERSONALE

5.5.1. 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.

5.5.2. 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:

- *Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)*
  Tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato (vedi *infra* art. 640 bis c.p.).

- *Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)*
  La linea di demarcazione tra l'ipotesi di Truffa aggravata per il conseguimento di erogazioni pubbliche (ex art. 640 bis c.p.) e quella di Indebita percezione di erogazioni a danno dello Stato (ex art. 316 ter c.p.) risiede nel tipo di condotta criminosa del reo che, nel secondo caso, si limita a presentare documenti falsi o ad omettere informazioni dovute; mentre nella prima ipotesi pone in essere artifizi o raggiri che provocano l'induzione in errore della Pubblica Amministrazione.
  Tale reato può realizzarsi, ad esempio nel caso in cui, nella predisposizione di documenti o dati per il finanziamento di piani formativi annuali e pluriennali si forniscano alla P.A. informazioni non veritiere

o rendicontazione supportate da documentazione artefatta

- *Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)*
- *Concussione (art. 317 c.p.)*
- *Corruzione (art. 318, 319 c.p.)*
- *Istigazione alla corruzione tra privati (art. 2635 bis c.c.)*
  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.
- *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)*
  Tale processo potrebbe realizzarsi, in concreto, anche in caso di illecito controllo delle comunicazioni dei dipendenti. Il reato si realizza, ad esempio, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente, con il vantaggio concreto dell'ente di appartenenza.
- *Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)*
  Il reato in parola potrebbe realizzarsi laddove gli apicali installino apparecchiature atte ad intercettare, ovvero nel caso di installazione di apparecchiature atte a intercettare le comunicazioni telematiche o informatiche dei dipendenti.
- *Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)*
  Tale processo potrebbe realizzarsi, in concreto, in caso di ricorso a atti di concorrenza sleale Art. 2598 c.c. quali lo Storno o distrazione di dipendenti di fornitori o competitor.
- *Intermediazione illecita e sfruttamento del lavoro (art. 603bis c.p.)*
  Costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

- la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
- la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
- la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro.

- *Omicidio colposo (art. 589 c.p.)*
- *Lesioni personali colpose (art. 590 co. 3 c.p.)*
- *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)*
  In concreto è ipotizzabile in via esemplificativa il caso di dipendenti/distaccati, sui quali si faccia indebita pressione utilizzando la condizione di soggezione in cui si trovano e prospettando loro vantaggi o svantaggi indebiti, rispettivamente in caso di adesione o mancata adesione alle richieste della Società.
- *Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25 duodecies D.Lgs 231/01)*
  Il reato potrebbe realizzarsi laddove la Società impiegasse alle proprie dipendenze lavoratori stranieri privi di permesso di soggiorno regolare e/o in corso di validità. A tal riguardo dovrà farsi riferimento

anche a lavoratori formalmente non inquadrati come dipendenti della Società, ma che potrebbero rivendicare l'accertamento e/o la costituzione del rapporto di lavoro (ad es. somministrazioni irregolari e altre ipotesi previste dalla legge).

5.5.3. 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 quanto segue:

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 è previsto il coinvolgimento di una pluralità di soggetti con ruoli distinti (propositivi, autorizzativi, di controllo), per evitare un'eccessiva concentrazione del potere decisionale in capo ad una persona, tali da garantire:
  - la tracciabilità delle fonti dei CV (domande spontanee, agenzie di selezione, ecc.);
  - adozione meccanismi oggettivi e trasparenti idonei a verificare il possesso di requisiti attitudinali e professionali adeguati in relazione alla posizione da ricoprire.
  - 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.
- in fase di **formulazione dell'offerta di assunzione**, sono previste le seguenti attività:
  - verifica che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti a lui assegnati;
  - verifica che il contratto di assunzione sia sottoscritto da persona dotata di idonea procura in tal senso;
  - verifica, in caso di assunzione di personale extracomunitario, della regolarità del permesso di soggiorno;
  - richiesta al candidato di un kit di documenti prima della sua assunzione al fine di verificare l'esistenza di adeguati requisiti etici e morali (CV aggiornato, titolo di studio, dichiarazione sostitutiva casellario giudiziale e carichi pendenti).
- in fase di **assunzione**, devono essere previste le seguenti attività:
  - il responsabile HR consegna al nuovo assunto il badge, l'organigramma, il mansionario (caratteristiche della funzione e delle mansioni da svolgere), elementi normativi e retributivi, come regolati dal CCNL e da eventuali contratti aziendali, le regole generali di sicurezza e quelle sul luogo di lavoro, l'informativa sul trattamento dei suoi dati personali, l'autorizzazione al trattamento dei dati per il ruolo ricoperto e i relativi rischi associati (documento "Dotazione dipendente");
  - impegno del neoassunto, mediante apposizione di sottoscrizione, al rispetto del Codice Etico e del Modello Organizzativo ex D.Lgs. 231/2001 della Società;
  - esecuzione degli obblighi nei confronti degli enti pubblici di riferimento (Inps, Inail);
  - archiviazione in formato cartaceo/informatico dei dati/documenti/atti predisposti nel corso delle attività (CV, esito del colloquio, valutazioni, lettere di assunzione, ecc.), per assicurare la tracciabilità del processo di selezione ed assunzione;

PROCESSO DI GESTIONE DEL PERSONALE:

- definizione formale degli obiettivi basata su criteri di specificità, oggettività, misurabilità, realizzabilità;
- gestione degli eventuali piani di incentivazione del personale con particolare riferimento alla definizione di: (i) livelli professionali di applicazione; (ii) obiettivi da assegnare; (iii) modalità di calcolo della componente variabile della retribuzione;
- erogazione formazione obbligatoria in materia di: compliance a Modello 231, salute e sicurezza dei luoghi di lavoro, sicurezza delle informazioni e privacy. Per ciascuna delle attività del Piano di formazione continuo, si evidenzia:
  - la frequenza e l'obbligatorietà, effettiva, della partecipazione;
  - il contenuto dei programmi formativi ed il loro aggiornamento;
  - il corretto svolgimento delle attività;
  - l'analisi dei questionari compilati dal personale
  - la tracciabilità della documentazione didattica.
- sviluppo di specifici programmi formativi, acquisizione certificazioni professionali, coinvolgendo i responsabili delle strutture competenti, compatibilmente con le risorse economiche di budget all'uopo destinate;
- pianificazione di risorse sulle attività di business in sostituzione temporanea a quelle impegnate in training;
- archiviazione in formato cartaceo/informatico dei dati/documenti/atti predisposti nel corso delle attività, per assicurare la tracciabilità del processo di formazione, progressioni di carriera, assegnazione di bonus, ecc.;

PROCESSO DI AMMINISTRAZIONE DEL PERSONALE:

- i rapporti con i fornitori di servizi professionali per le elaborazioni delle partite stipendiali prevedeono 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.
- sono codificate le regole per la rilevazione delle presenze e la verifica delle stesse;
- sono codificate le regole per le richieste e il rilascio delle autorizzazioni per ferie e permessi e le modalità di comunicazioni di malattie e aspettative;
- sono codificate le regole per le trasferte, le necessarie autorizzazioni e la definizione delle tipologie di spese rimborsabili, dei limiti di importo relativi alle varie tipologie di spese e delle relative modalità di rendicontazione;
- l'assegnazione di strumenti di lavoro (ad esempio autovetture, sim, telefoni, pc) prevede l'utilizzo di 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;
- sono stabilite le modalità di restituzione dei beni in caso di cessazione del rapporto di lavoro;
- sono definite modalità specifiche per la gestione dei casi di furto o smarrimento dei beni assegnati, garantendo la tracciabilità delle motivazioni di eventuali nuove assegnazioni.
- è costantemente monitorato il rispetto di tutte le disposizioni normative in materia di lavoro e di tutela della Privacy. La Società attua tutti i comportamenti e le decisioni necessarie, e relativi controlli, affinché non si verifichino fenomeni di:
  - minaccia, violenza o intimidazione;
  - retribuzioni palesemente difformi dai Contratti Collettivi Nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative;
  - retribuzioni palesemente sproporzionate rispetto alla quantità e qualità del lavoro prestato;

- violazione della normativa relativa: 1) all'orario di lavoro imponendo anomali o inusuali ritmi di lavoro; 2) ai periodi di riposo; 3) al riposo settimanale; 4) all'aspettativa obbligatoria; 5) alle ferie; 6) alle misure in materia di sicurezza, salute ed igiene sul luogo di lavoro;
- utilizzo di metodi di sorveglianza, diretta o a distanza;
- somministrazione di lavoro abusiva o fraudolenta;
- appalti in assenza dei requisiti normativi con il rischio di commettere il reato c.d. di "pseudo-appalto";
- distacco fittizio di un lavoratore, anche in assenza dei requisiti normativi con il rischio di commettere il reato c.d. di "distacco illecito".

5.6. AMMINISTRAZIONE, FINANZA, CONTROLLO ED OPERAZIONI SUL CAPITALE

5.6.1. ATTIVITÀ A RISCHIO

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

a) Gestione della finanza e della tesoreria e rapporti con istituti bancari e finanziari
b) Amministrazione e contabilità (rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni e in altri documenti di impresa, aggiornamento del piano dei conti, fatturazione attiva, fatturazione passiva, gestione del credito)
c) Gestione degli adempimenti fiscali
d) Formazione del bilancio e delle relazioni infrannuali (valutazioni e stime di poste di bilancio)
e) Gestione delle trasferte, delle note spese e delle spese di rappresentanza
f) Rapporti con i Soci, il CdA e il Collegio Sindacale
g) Controllo di gestione (piano pluriennale, budget, consuntivi infrannuali, gestionali, analisi scostamenti obiettivi/risultati, reporting gestionali)

5.6.2. 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:

➢ ***Reati tributari (Art. 25 quinquiesdecies D.lgs. 231/01)***

- *Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti* - Art. 2 D.Lgs.n.74:
  Il reato è a consumazione istantanea e si realizza nel momento della presentazione della dichiarazione dei redditi. La mera predisposizione e la registrazione nelle scritture contabili obbligatorie dei documenti attestanti operazioni inesistenti sono condotte meramente preparatorie e non punibili, nemmeno a titolo di tentativo.
- *Dichiarazione fraudolenta mediante altri artifici - Art. 3 D.Lgs.n.74:*
  Il reato è a consumazione istantanea e si realizza nel momento della presentazione della dichiarazione dei redditi. Il fatto si considera commesso avvalendosi di documenti falsi quando questi sono registrati nelle scritture contabili obbligatorie o detenuti a fini di prova nei confronti dell'Amministrazione Finanziaria.
- *Emissione di fatture o altri documenti per operazioni inesistenti - Art. 8 D.Lgs.n.74:*

Ad es. la contabilizzazione di fatture false di fornitori per prestazioni inesistenti, o ancora il pagamento di fatture fittizie (in tutto o in parte) per creare delle "disponibilità".

- *Occultamento o distruzione di documenti contabili - Art. 10 D.Lgs.n.74:*
  Il reato è considerato perfezionato nel momento in cui l'occultamento o la distruzione delle scritture contabili provocano, come effetto diretto, l'impossibilità di ricostruire la situazione reddituale o la ricostruzione del volume d'affari del contribuente. Ad es. l'omessa contabilizzazione di poste.
- *Sottrazione fraudolenta al pagamento di imposte -Art.11 D.Lgs.n.74:*
  La condotta punita è connotata dallo scopo di rendere inefficace, per sé o altri, la procedura di riscossione coattiva o di ottenere un pagamento inferiore delle somme complessivamente dovute, mediante atto simulato di alienazione o altri atti fraudolenti sui propri o altrui beni.
- *Dichiarazione infedele -Art.4 D.Lgs. 74/2000*
  ad esempio, la società falsifica la dichiarazione ai fini dell'imposta sul valore aggiunto, superando la soglia limite imposta dal legislatore e ottenendo fraudolentemente un risparmio;
- *Omessa dichiarazione -Art.5 D.Lgs. 74/2000*
  ad esempio, la società omette di presentare la dichiarazione ai fini dell'imposta sul valore aggiunto, superando la soglia limite imposta dal legislatore e conseguendo un risparmio;
- *Indebita compensazione - Art.10 quater D.Lgs. 74/2000*
  ad esempio, la società produce documentazione falsa al fine di beneficiare in compensazione di un credito inesistente o non spettante, non superando la soglia limite imposta dal legislatore e conseguendo un risparmio.

Questi ultimi tre reati tributari rilevano, ai fini della responsabilità amministrativa dell'ente, esclusivamente qualora commessi **nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.**

Tali reati potrebbero portare alla costituzione di "**disponibilità**" strumentali alla realizzazione di altri reati:

- *Corruzione, corruzione tra privati ed istigazione alla corruzione tra privati (art. 2635 bis c.c.)*
  Offrendo o consegnando denaro o altra utilità ai soggetti di altre società private (ad es. fornitori)
- *Corruzione per l'esercizio della funzione e/o corruzione per un atto contrario ai doveri d'ufficio (art. 318, 319 c.p.)*
  Offrendo o consegnando denaro o altra utilità al pubblico ufficiale, o all'incaricato di pubblico servizio per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente).

Inoltre, nel caso in cui vengano falsificati, con l'obiettivo di ottenere un profitto i **dati delle dichiarazioni fiscali/contributive:**

- *Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)*
  Gli artifici o raggiri richiesti dalla fattispecie si concretizzano nella falsificazione dei dati delle dichiarazioni fiscali/contributive per ottenere finanziamenti pubblici o erogazioni pubbliche (contributi, mutui agevolati ovvero altre erogazioni dello stesso tipo).

➢ ***Reati societari (art. 25-ter D.lgs. 231/01) (da inserire anche nel paragrafo SOCI)***

- *False comunicazioni sociali e false comunicazioni sociali in danno della società, dei soci e dei creditori (artt. 2621 e 2621-bis c.c.)*
  A titolo meramente esemplificativo:

- la valutazione di bilancio ha ad oggetto dati fattuali inesistenti;
- nella Nota Integrativa è dichiarato che la valutazione è stata eseguita secondo un determinato criterio che, tuttavia, è applicato in modo scorretto o del tutto parziale;
- l'attribuzione come costi accessori di spese che non possono essere ricomprese in tale tipologia o oneri finanziari estranei alla realizzazione del bene;
- vi è disparità fra i criteri di valutazione iscritti in Nota Integrativa e le stime compiute in bilancio (cosiddetto criterio della "difformità fra prescelto e dichiarato").

- *Indebita restituzione dei conferimenti (art. 2626 c.c.)*
  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 (art. 2627 c.c.)*
  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, attuata anche mediante la falsificazione, l'alterazione o la distruzione dei documenti di rendicontazione.
- *Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)*
  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.
- *Operazioni in pregiudizio dei creditori (art. 2629 c.c.)*
  determinazione di poste valutative di bilancio non conformi alla reale situazione economica, patrimoniale e finanziaria delle Società, oppure inesistenti o di valore difforme da quello reale.
- *Formazione fittizia del capitale (art. 2632 c.c.)*
  Il reato in esame potrebbe configurarsi nel caso in cui gli amministratori e i soci conferenti formino o aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, mediante sottoscrizione reciproca di azioni o quote, altresì attraverso una sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.
- *Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza (art. 2638 c.c.)*
  Il reato in esame potrebbe realizzarsi nel caso in cui gli amministratori, ovvero i soggetti apicali della Società ovvero gli addetti agli organi di controllo, pongano in essere condotte di ostacolo all'esercizio delle funzioni delle Autorità di Vigilanza, a titolo esemplificativo al fine di evitare alla Società sanzioni o altre conseguenze pregiudizievoli.
- *Impedito controllo (2625 co. 2 c.c.)*
  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.

In ultimo non si possono escludere:

➢ ***Ricettazione, riciclaggio e impiego di denaro, beni o altre utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies D.lgs.231/01)***

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.

5.6.3. PROTOCOLLI DI CONTROLLO SPECIFICI

a) Gestione della finanza e della tesoreria e rapporti con istituti bancari e finanziari

- modalità operative per assicurare che ciascun incasso e/o pagamento debba essere associato ad un corrispondente documento contabile (es. fattura attiva o fattura passiva), al fine di assicurare la corretta tenuta della contabilità di cassa;

- segregazione delle funzioni tra chi provvede all'esecuzione dei pagamenti e chi provvede alla verifica di coerenza del pagamento con la prestazione o i servizi ricevuti;

- autorizzazione dei pagamenti e di qualsiasi altra uscita di cassa da parte delle competenti funzioni sulla base delle procure assegnate, previa acquisizione della documentazione di supporto debitamente verificata e validata;

- verifica preventiva affinchè le transazioni finanziarie siano effettuate, nel rispetto delle normative applicabili, nei confronti di controparti effettivamente esistenti e per prestazioni effettivamente ricevute;

- verifica di correttezza e completezza delle operazioni di pagamento anche finalizzate ad accertare che: i) l'importo sia corrispondente a quanto effettivamente dovuto e previsto contrattualmente; ii) vi sia corrispondenza tra l'appoggio bancario indicato in fattura e quello presente in anagrafica; iii) l'operazione sia stata debitamente autorizzata;

- obbligo di: i) utilizzare operatori finanziari abilitati, in conformità con le normative applicabili, all'erogazione di servizi in materia bancaria e creditizia o comunque abilitati allo svolgimento di attività di incasso e pagamenti; ii) effettuare i pagamenti solo a favore della controparte designata contrattualmente, e nel Paese in cui la controparte ha la propria sede legale o nel Paese in cui la fornitura di beni e servizi viene eseguita;

- determinazione di limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative. Il superamento dei limiti quantitativi di spesa assegnati può avvenire solo ed esclusivamente per comprovati motivi di urgenza e in casi eccezionali: in tali casi è previsto che si proceda alla sanatoria dell'evento eccezionale attraverso il rilascio delle debite autorizzazioni;

- divieto di utilizzo del contante, ad eccezione dei casi espressamente disciplinati nella procedura che regola l'utilizzo o di altro strumento finanziario al portatore per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziaria, nonché divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;

- completezza, accuratezza e veridicità delle registrazioni di incassi, pagamenti e delle operazioni di tesoreria, previa verifica della completezza e accuratezza della documentazione a supporto;

- esecuzione delle riconciliazioni dei saldi (ad es. conti correnti bancari, clienti e fornitori terzi più rilevanti);

- definizione delle tipologie di spesa che possono essere sostenute a mezzo cassa e monitoraggio delle stesse;

- formale autorizzazione, da parte di adeguati livelli organizzativi, delle operazioni di apertura di un nuovo conto corrente della Società o di finanziamento e delle modifiche/chiusura dei conti correnti della Società;

- chiara individuazione dei soggetti autorizzati ad operare sui conti correnti della Società;

- limitazione degli accessi al sistema di remote banking, ai fini delle movimentazioni sui conti correnti della Società, tramite l'assegnazione di username e password dispositive;

- formale autorizzazione, da parte di adeguati livelli organizzativi e in base alle strategie aziendali adottate, delle operazioni di effettuazione di un investimento finanziario e chiara individuazione dei soggetti autorizzati ad operare sugli investimenti finanziari della Società;

- nel ricercare le controparti con le quali stipulare i finanziamenti, la funzione competente si rivolge esclusivamente a primarie controparti bancarie. In particolare, 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.

- le decisioni relative alle politiche di finanza strategica ed operativa (es. accensione o estinzione di contratti di finanziamento, apertura/chiusura di conti correnti bancari) sono adeguatamente documentate ed autorizzate secondo il sistema di deleghe vigente;

- tutti gli atti di disposizione che comportano lo spostamento o l'impiego di fondi sui conti correnti intestati alla Società sono adeguatamente documentati ed autorizzati;

- la funzione competente garantisce evidenza documentale delle diverse fasi di negoziazione del contratto di finanziamento, da cui risultino le controparti contattate e le condizioni che sono state offerte;

- tutti i contratti di finanziamento sono autorizzati da un soggetto aziendale dotato di idonei poteri e, preliminarmente, dal Consiglio d'Amministrazione, ove necessario per le operazioni maggiormente rilevanti;

- nella gestione delle operazioni di finanziamento, viene verificata la coerenza dei tassi applicati con i valori medi di mercato.

b) Amministrazione e contabilità (rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni e in altri documenti di impresa, aggiornamento del piano dei conti, fatturazione attiva, fatturazione passiva, gestione del credito)

Si premette che ogni operazione deve essere sempre verificabile, documentata, coerente e congrua al fine di assicurare una "rappresentazione veritiera e corretta" del bilancio.

L'indicazione di qualsiasi fatto materiale non corrispondente al vero di qualsivoglia entità può integrare il reato di false comunicazioni sociali, quantomeno nella forma attenuata.

Con specifico richiamo al Codice Etico, si sottolinea che l'Azienda è consapevole dell'importanza della trasparenza, accuratezza, tracciabilità e completezza delle informazioni contabili e si adopera per disporre di un sistema amministrativo/contabile affidabile nel rappresentare correttamente i fatti di gestione e nel fornire gli strumenti per identificare, prevenire e gestire, nei limiti del possibile, rischi di natura finanziaria e operativa, nonché frodi a danno proprio e di terzi, tramite:

- identificazione dei soggetti deputati alla gestione della contabilità e alla predisposizione ed approvazione delle comunicazioni sociali o documentazione equivalente;

- l'abilitazione ad effettuare le registrazioni contabili è concessa in ragione delle responsabilità e delle mansioni svolte da ciascun utente, mediante la definizione di specifici profili di accesso al sistema gestionale-contabile;

- accesso ai sistemi informativi per la gestione della contabilità e la predisposizione del bilancio limitato a soggetti preventivamente abilitati ed attraverso User-ID e password;

- definizione di un sistema di archiviazione delle registrazioni contabili che ne permetta la tracciabilità;

- identificazione dei soggetti responsabili di effettuare ed approvare le scritture contabili manuali e definizione delle modalità di archiviazione e tracciabilità della relativa documentazione a supporto;

- adozione di procedure contabili, costantemente aggiornate, indicanti con chiarezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro trasmissione alle funzioni responsabili. La rilevazione, la trasmissione e l'aggregazione delle informazioni contabili finalizzate alla predisposizione delle comunicazioni sociali avviene esclusivamente tramite modalità che possano garantire la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei soggetti che inseriscono i dati nel sistema;

- autorizzazione di eventuali modifiche ai criteri di contabilizzazione dalla funzione Amministrazione;

- corretta determinazione delle comunicazioni sociali, affinché siano rispondenti a quanto previsto/ richiesto dalla normativa applicabile alla Società;

- comunicazione immediata all'Organismo di Vigilanza di richieste da parte di chiunque di ingiustificate variazioni dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure operative della Società.

Con particolare riferimento alla ***capitalizzazione degli asset*** e alla ***gestione dei piani di ammortamento***, le procedure e le prassi vigenti garantiscono il rispetto dei seguenti protocolli specifici di comportamento e di controllo:

- adozione di un registro dei beni ammortizzabili (libro dei cespiti) all'interno del quale sono censiti tutti gli asset di cui la Società dispone, in cui siano indicati anche gli asset presso i terzi;

- definizione dell'iter approvativo per autorizzare l'inserimento, la modifica o la cancellazione di un asset;

- verifica e approvazione della classificazione di un nuovo asset quale "bene pronto all'uso" (per il quale il processo di ammortamento contabile e fiscale ha inizio a seguito dell'entrata merce) o "bene che richiede ulteriori lavorazioni" (immobilizzazioni in corso per le quali il processo di ammortamento contabile e fiscale ha inizio in un momento successivo all'entrata merce);

- monitoraggio delle immobilizzazioni in corso al fine di identificare prontamente e correttamente gli asset ultimati per i quali può essere avviato il processo di ammortamento;

- definizione delle modalità di applicazione delle corrette quote di ammortamento annuali, sulla base delle aliquote civilistiche e fiscali definite in fase di registrazione dell'asset;

  Inoltre, ai fini della tenuta e custodia della **documentazione obbligatoria** e delle scritture contabili, le procedure e le prassi vigenti garantiscono la definizione delle responsabilità, i termini e le modalità di archiviazione della documentazione fiscale e contabile obbligatoria, tra cui:

  - il libro giornale;
  - fatture attive, fatture passive, note di credito e note di debito;
  - libro cespiti e registro dei beni ammortizzabili;
  - registri IVA;
  - corrispondenza commerciale, Ordini e Contratti di Acquisto, Contratti di Vendita, etc.;
  - scritture ausiliarie quali documenti di trasporto di beni ricevuti e spediti, etc.;

Fatturazione passiva

- Qualsiasi pagamento può essere eseguito solo se corrispondente ad una specifica e autorizzata documentazione di acquisto (contratto, ordine di acquisto e fattura) e viene autorizzato secondo il vigente sistema di deleghe e procure. I livelli autorizzativi previsti per l'autorizzazione dei pagamenti a fornitori, ai dipendenti e ai terzi in genere risultano chiaramente definiti e tracciabili;

- tutti i pagamenti sono disposti tramite bonifico bancario o altra modalità che ne garantisca la tracciabilità;

- per disporre un pagamento è prevista formale autorizzazione - mediante rilascio di benestare a sistema o altra modalità prevista dalle procedure vigenti - da parte di un responsabile, incaricato in base al sistema di deleghe interne;

- è accertata la completezza delle informazioni presenti in fattura, tramite verifica supportata da evidenze formali (coerenza tra la quantità prevista nel documento entrata merce e la quantità presente in fattura;

- le disposizioni di bonifico sono autorizzate formalmente da soggetto dotato di idonei poteri (che, nel caso di pagamenti tramite remote banking, deve disporre di credenziali di accesso riservate e personali);

- ove previsto dalla normativa vigente in materia di tracciabilità dei flussi finanziari, i pagamenti sono effettuati solo sui conti correnti "dedicati" comunicati per iscritto dalla parte ricevente;

- in caso di pagamento su conti esteri, sono previsti controlli finalizzati a verificare che: 1) non si tratti di conti c.d. "cifrati"; 2) il conto corrente non risieda presso uno Stato considerato "a rischio";

- i pagamenti effettuati con modalità differenti dal bonifico o giroconto bancario sono adeguatamente documentati ed autorizzati;

- vige il divieto di cedere il credito a terzi salvo preventiva approvazione di Teleconsys;

- è verificata e costantemente e monitorata la coerenza contabile tra fatture ed incassi;

Fatturazione attiva

- ciascun incasso è abbinato ad una specifica commessa, in cui trova adeguata giustificazione;

- le operazioni che comportano flussi in entrata sono effettuate con mezzi idonei a garantire la tracciabilità dell'operazione (es. causale espressa, indicazione del soggetto ordinante, ecc.);

- tutte le fatture attive sono emesse a fronte di prestazioni di servizi resi o a fronte di beni forniti a clienti e sono adeguatamente documentate ed autorizzate secondo il vigente sistema di deleghe e procure;

- ai fini del recupero del credito, è sempre identificato un referente aziendale dotato delle deleghe necessarie per rappresentare la Società o per coordinare l'azione di eventuali professionisti esterni;

- sono stabilite le modalità (ad es. sollecito verbale, diffida scritta) attraverso le quali attuare la procedura di recupero del credito;

- sono formalmente identificati i soggetti autorizzati a concordare un eventuale piano di rientro;

- sono archiviati, mediante supporti cartacei o elettronici, tutti i documenti relativi al procedimento di recupero del credito.

Inoltre, 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".

c) Gestione degli adempimenti fiscali

- formale identificazione dei soggetti deputati ad intrattenere i rapporti e a rappresentare la Società nei confronti dell'Amministrazione Finanziaria, anche in sede di ispezioni ed accertamenti da parte di quest'ultima;

- esistenza di segregazione tra chi effettua il calcolo delle imposte, e predispone i modelli di versamento e dichiarativi e chi approva il pagamento delle imposte e la trasmissione dei Modelli stessi all'Amministrazione Finanziaria;

- presenza di controlli, anche con il supporto di soggetti autonomi ed indipendenti, per verificare la correttezza e la completezza della compilazione dei prospetti delle dichiarazioni fiscali, prima di sottometterli alla firma autorizzativa;

- formale sottoscrizione, nel rispetto delle responsabilità in essere, dei modelli di versamento e dichiarativi;

- costante monitoraggio dell'evoluzione della normativa di riferimento e delle tempistiche da rispettare per le comunicazioni / denunce / adempimenti nei confronti dell'Amministrazione Finanziaria;

- definizione, supportata da evidenze formali, delle modalità e dei criteri per la determinazione delle imposte, correnti e differite, nel rispetto della normativa fiscale vigente;

- presenza di un prospetto di monitoraggio ex post che rappresenti i fatti rilevanti che caratterizzano la fiscalità del periodo e che permetta la ricostruibilità e la tracciabilità a posteriori;

- tutti gli atti, le richieste e le comunicazioni formali che hanno come controparte l'Amministrazione Finanziaria e gli enti certificatori sono gestiti, autorizzati e firmati solo da coloro che sono dotati di idonei poteri in base alle norme interne;

- tracciabilità, anche attraverso i sistemi informativi aziendali, di tutte le dichiarazioni, la reportistica relativa alla gestione degli adempimenti fiscali;

- qualora le operazioni oggetto del presente protocollo siano date in outsourcing, la Società comunica al fornitore del servizio il proprio Codice di Comportamento e il proprio Modello, dei cui principi richiede il rispetto attraverso opportune clausole contrattuali.

d) Formazione del bilancio e delle relazioni infrannuali (valutazioni e stime di poste di bilancio)

L'attività sensibile in esame riguarda il processo di chiusura contabile finalizzato alla predisposizione del bilancio annuale e all'emissione dei relativi documenti contabili societari.

In particolare, le procedure e le prassi vigenti garantiscono il rispetto dei seguenti Protocolli specifici di comportamento e di controllo:

- nell'attività di contabilizzazione dei fatti relativi alla gestione della Società, vengono osservate le regole di corretta, completa e trasparente registrazione, secondo:
    - criteri obiettivi e valutativi, determinati dalla disciplina civilistica (tra cui l'art. 2426 c.c.), coerenti ed indiscussi sul piano tecnico e normativo;
    - Direttive e Regolamenti comunitari;
    - decisioni individuabili e tracciate;
    - prassi universalmente accettate e standard elaborati a livello internazionale (ad es.: IAS/IFRS).
- è garantita la tempestività, l'accuratezza e il rispetto del principio di competenza nell'effettuazione delle registrazioni contabili;
- è assicurato che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima e coerente con la documentazione di riferimento;
- è assicurata la verifica e l'aggiornamento sul rispetto dei principi contabili e delle esigenze di informativa imposte dalle disposizioni normative e regolamentari applicabili;
- è garantita la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte nel processo di chiusura contabile e di predisposizione del bilancio e delle situazioni contabili infrannuali;
- tutte le attività finalizzate alla formazione del bilancio e delle situazioni contabili infrannuali, e delle altre comunicazioni sociali, sono improntate a un comportamento corretto, trasparente e collaborativo al fine di fornire al Socio ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- le comunicazioni con le varie Direzioni/Funzioni aziendali finalizzate alla raccolta di dati e informazioni per la chiusura contabile avvengono in forma scritta, nel rispetto della tempistica prevista;
- il calcolo per la definizione delle poste estimative/valutative e delle imposte risulta sempre tracciabile;
- le scritture di chiusura, assestamento e rettifica e le poste estimative/valutative sono effettuate nel rispetto dei principi contabili adottati e sono sottoposte a verifica e autorizzazione da parte del responsabile prima di essere registrate;
- la bozza degli schemi di bilancio, delle note illustrative e della relazione sulla gestione sono verificate dal Responsabile Amministrazione, Finanza e Controllo;
- le bozze dei progetti di bilancio e delle situazioni contabili infrannuali sono presentate all'Amministratore Delegato che ne autorizza la presentazione al Consiglio di Amministrazione;

- l'Amministratore Delegato firma l'attestazione sull'adeguatezza e l'effettiva applicazione delle procedure amministrativo-contabili;

- la bozza del progetto di Bilancio è consegnata a tutti i componenti del Consiglio di Amministrazione, con adeguato anticipo e con documentata certificazione dell'avvenuta consegna, prima della riunione per l'approvazione dello stesso, unitamente alle relazioni accompagnatorie redatte dal Collegio sindacale, nonché delle attestazioni e relazioni del Dirigente preposto alla redazione dei documenti contabili societari;

- sono consegnati all'Organismo di Vigilanza tutti i documenti contabili e di supporto alla redazione dei bilanci e ogni altra relazione, prospetto o comunicazione sociale prevista dalla legge.

e) Gestione delle trasferte, delle note spese e delle spese di rappresentanza

- autorizzazione preventiva all'esecuzione di trasferte da parte del responsabile gerarchico con rimborsi a piè di lista su presentazione di adeguati giustificativi;

- pre-definizione delle tipologie di spese rimborsabili, dei limiti di importo relativi alle varie tipologie di spese (ad esempio di viaggio, di soggiorno, ecc.), degli importi massimi e delle relative modalità di rendicontazione;

- attribuzione della responsabilità di verificare la coerenza tra le spese sostenute, le attività svolte e la documentazione di supporto;

- segregazione tra chi autorizza l'esecuzione di trasferte, chi verifica le note spese e chi ne autorizza il rimborso;

- definizione dei criteri di assegnazione delle carte di credito aziendali;

- definizione dei soggetti autorizzati a sostenere spese di rappresentanza;

- definizione dei criteri di accettabilità delle spese di rappresentanza, le quali comunque devono essere "moderate" e chiaramente destinate a facilitare le discussioni di lavoro.

f) Rapporti con i Soci, il CdA e il Collegio Sindacale

- 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;

- 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 gli incassi e i pagamenti derivanti da rapporti di acquisto o vendita di partecipazioni, 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;

- ripartire utili o acconti su utili effettivamente conseguiti e non destinati per legge a riserva;

- acquistare o sottoscrivere azioni proprie 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.

Nell'ambito della gestione delle operazioni straordinarie, le procedure e le prassi vigenti devono garantire il rispetto dei seguenti protocolli specifici di comportamento e di controllo:

- i ruoli e responsabilità delle unità coinvolte nello svolgimento delle attività operative;

- le modalità di coinvolgimento di advisor esterni nonché le modalità di accesso da parte di quest'ultimi ad informazioni e documentazione della Società e/o dell'operazioni straordinaria; la predisposizione di idonea documentazione a supporto dell'operazione, da parte delle funzioni aziendali proponenti o competente all'istruzione della pratica;

- la verifica preliminare da parte della funzione aziendale competente della completezza, inerenza e correttezza della documentazione di supporto dell'operazione, ai fini della registrazione contabile;

- il coinvolgimento della Funzione Fiscale affinché valuti i riflessi fiscali dell'operazione e l'eventuale necessità di pareri indipendenti;

- la previsione che ogni operazione straordinaria sia sottoposta e approvata dal Consiglio di Amministrazione della Società;

- la previsione, anche attraverso il supporto di eventuali Advisor specialistici, di attività di Due Diligence esterna (in caso di acquisizione) o interna (in caso di cessioni) sull'oggetto della compravendita. Il rapporto di Due Diligence deve contenere: (i) nominativi delle persone che hanno condotto le attività di due diligence; (ii) esami effettuati e i relativi esiti; (iii) deduzioni e raccomandazioni fatte; (iv) eventuali modifiche agli accordi da proporre alla controparte;

- la richiesta alla società di revisione e al Comitato di Controllo di un motivato parere sull'operazione, ove richiesto da normativa o ritenuto opportuno.

g) Controllo di gestione (piano pluriennale, budget, consuntivi infrannuali, gestionali, analisi scostamenti obiettivi/risultati, reporting gestionali)

- sono regolamentati i criteri e le modalità di elaborazione del budget e la conseguente regolare predisposizione di reporting infra-annuali con confronto tra dati consuntivi e budget, che rendono necessario, pertanto, un aggiornamento periodico del budget annuale;

- periodicamente viene eseguita la definizione e il monitoraggio del "Forecast", condiviso tra le diverse Funzioni aziendali interessate;

- il budget viene diffuso e comunicato a tutte le funzioni aziendali interessate, suddiviso per i singoli centri di costo;

- viene eseguito un monitoraggio periodico dei costi e la relativa analisi degli scostamenti.

5.7. GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO

5.7.1. ATTIVITÀ A RISCHIO

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;
- gestione emergenza epidemiologica Covid - 19

5.7.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le attività relative alla implementazione e gestione di sistemi di sicurezza e tutela dell'igiene dei luoghi di lavoro, espongono la Società ai rischi di commissione dei seguenti principali reati:

- *Omicidio colposo (art. 589 c.p.)*
- *Lesioni personali colpose (art. 590 co. 3 c.p.)*

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..

Inoltre, nell'ambito di verifiche cui Teleconsys può essere sottoposta o richieste di autorizzazioni, l'instaurazione di rapporti con pubblici ufficiali e/o incaricati di pubblico servizio potrebbero rilevare anche ai fini dei reati di:

- *Corruzione (art. 318, 319 c.p.)*
- *Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)*

5.7.3. PROTOCOLLI DI CONTROLLO SPECIFICI

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;

Si evidenzia che, in ragione dell'emergenza epidemiologica da Covid -19, il DVR della Società è stato opportunamente integrato dal "Protocollo di sicurezza anti-contagio", redatto in linea con le prescrizioni dettate da Confindustria nel documento "Prime indicazioni operative Giugno 2020" e s.m.i..

- *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.
Dal 2022 Teleconsys adotta un sistema di gestione per la salute e sicurezza sul lavoro certificato secondo la norma internazionale ISO 45001:2018.

5.8. AMBIENTE

5.8.1. ATTIVITÀ A RISCHIO

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati ambientali previsti dall'art. 25-undecies del Decreto e ritenuti ad essa applicabili:

a) Gestione della compliance ambientale
- l'attività di definizione, manutenzione ed attuazione del sistema di gestione ambientale nel suo complesso e del sistema procedurale;
- la gestione degli aspetti autorizzativi e gestione dei rapporti con le autorità
- la valutazione e la gestione delle intervenute modifiche riconducibili a fattori esogeni di tipo normativo ovvero endogeni riferite a modifiche organizzative, strutturali, operative;
- il monitoraggio periodico delle prestazioni ambientali, svolgimento attività di audit e identificazione misure correttive e programmi ambientali

b) Gestione dei fornitori a rilevanza ambientale
- la selezione, la qualifica e la valutazione dei fornitori di beni e servizi con un potenziale impatto sull'ambiente

c) Gestione della Sede,
- la gestione e il monitoraggio delle sedi della Società finalizzata al monitoraggio delle emissioni, degli scarichi idrici, , ecc.;
- la gestione delle attività di manutenzione degli impianti e di eventuali strumentazioni aziendali volte alla mitigazione degli impatti ambientali

d) Gestione smaltimento rifiuti
- monitoraggio delle attività di conferimento dei rifiuti ai trasportatori, anche terzi.

Teleconsys nel 2022 ha adottato un sistema di gestione ambientale certificato secondo la **norma UNI ISO 14001:2015**, per sviluppare e migliorare in modo sistematico le proprie prestazioni ambientali nell'ambito della sostenibilità, fissando gli obiettivi generali che la stessa si è proposta di raggiungere e le procedure necessarie a tal fine, da comunicare adeguatamente ai dipendenti ed alle parti interessate e da aggiornare periodicamente.

Nel **Bilancio di sostenibilità**, redatto a partire dall'annualità 2021, sono rendicontati, in conformità ai GRI Standard, gli aspetti rilevanti che riflettono anche l'impatto significativo ambientale dell'organizzazione. In questo contesto, l'impatto si riferisce agli effetti, positivi e/o negativi, che l'organizzazione ha sull'ambiente, anche rispetto alle aspettative, interessi e valutazioni dei propri stakeholder.

5.8.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

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.
Tuttavia, in Teleconsys non vengono svolte attività che potrebbero, anche solo potenzialmente, esporre la Società alla commissione (anche in concorso) della maggior parte dei reati ivi richiamati, ad eccezione di:

➢ ***Inquinamento ambientale (art. 452-bis c.p.)***

➢ ***Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)***

Il reato potrebbe configurarsi laddove la Società cagionasse una compromissione o un deterioramento significativo e misurabile dell'acqua e dell'aria o di porzioni significative del suolo o del sottosuolo nello svolgimento delle proprie attività. Ad esempio, nel caso in cui a seguito di un 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 di un ecosistema, ovvero effetti lesivi su un elevato numero di persone o esposizione di un numero elevato di persone a pericolo.

➢ ***Reati connessi alla gestione dei rifiuti, previsti dall'art. 256, commi 1, 3, 5 e 6, D.Lgs. 152/2006***

5.8.3. PROTOCOLLI DI CONTROLLO SPECIFICI

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.

Inoltre:

- 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.

Nell'ambito della gestione delle attività sensibili, in cui, potenzialmente, potrebbero essere commessi i reati ambientali previsti dall'art. 25-undecies del Decreto, trovano applicazione i protocolli specifici di prevenzioni definiti per ciascuna attività, che prevedono quanto segue:

Gestione della compliance ambientale

Sono stabilite procedure atte a garantire:

- 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, con riferimento a: i) rispetto delle regole in materia ambientale anche da parte dei terzi che operano presso Teleconsys; ii) efficacia delle regole adottate; iii) conformità alla normativa ambientale delle attività; iv) definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate nel corso dell'attività di auditing.

-

Gestione dei fornitori a rilevanza ambientale

Le procedure prevedono:

- verifica preliminare dei requisiti tecnico-professionali in capo ai fornitori;
- previsione di clausole contrattuali che impongano il rispetto delle normative ambientali applicabili e, ove necessario, delle procedure definite dalla Società, nonché del rispetto dei principi generali contenuti nel Modello e nel Codice Etico;
- previsione di attività di audit sui fornitori;
- previsione della valutazione delle performance dei fornitori.

Gestione della Sede

Sono stabilite procedure che garantiscono:

- 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;
- 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;
- la valutazione dell'impatto ambientale conseguente a modifiche strutturali o organizzative riguardanti la sede operativa;
- interventi di manutenzione periodica e programmata sugli scarichi e sui filtri degli impianti di condizionamento e conservazione della documentazione relativa alle attività di manutenzione

eseguite.

Gestione smaltimento rifiuti

Sono stabilite procedure atte a garantire:

- la corretta caratterizzazione e classificazione dei rifiuti;
- la corretta gestione degli adempimenti necessari al trasporto dei rifiuti dal momento della consegna al trasportatore fino al conferimento finale allo smaltitore (gestione dei formulari e dei registri carico/scarico, gestione SISTRI);
- 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.

5.9. RAPPORTI CON I SOCI, COLLEGIO SINDACALE E SOCIETÀ DI REVISIONE

5.9.1. 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:

a) Gestione dei rapporti con il Socio, Collegio Sindacale e Società di revisione
b) Gestione degli adempimenti relativi al funzionamento degli organi societari
c) Gestione delle operazioni societarie straordinarie (es. acquisizione di quote, di partecipazione in società del medesimo business)
d) Tutela dell'integrità di beni giuridici della Società

5.9.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

La gestione dei rapporti con i Soci e le Società partecipate potrebbe risultare strumentale alla commissione dei seguenti reati:

- *Corruzione (art. 318, 319 c.p.)*
  Laddove si assicurino favori di qualsiasi genere a soggetti appartenenti a società private o ad enti pubblici, che siano incaricati di gestire i rapporti contrattuali intercorrenti con la Società, tali da poter influenzare il loro libero convincimento nello svolgimento della loro attività.
- *False comunicazioni sociali e false comunicazioni sociali in danno della società, dei soci e dei creditori (artt. 2621 e 2621-bis c.c.)*
  Il reato in esame potrebbe configurarsi in concorso con amministratori, sindaci, ovvero il preposto al bilancio, esponendo nelle comunicazioni sociali previste dalla legge fatti materiali rilevanti non rispondenti al vero, ovvero omettano fatti materiali rilevanti la cui comunicazione è imposta dalla legge.
- *Indebita restituzione dei conferimenti (art. 2626 c.c.)*
  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 (art. 2627 c.c.)*
  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 o quote sociali o della società controllante (art. 2628 c.c.)*
  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.

- *Operazioni in pregiudizio dei creditori (art. 2629 c.c.)*
  Qualora, in violazione delle disposizioni di legge a tutela dei creditori, siano effettuate dai soci riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.
- *Formazione fittizia del capitale (art. 2632 c.c.)*
  Qualora i soci conferenti formino o aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, mediante sottoscrizione reciproca di azioni o quote, oppure attraverso una sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti o del patrimonio della società nel caso di trasformazione.
- *Corruzione ed istigazione alla corruzione tra privati (art. 2635-bis c.c.)*
  Nel caso in cui un esponente della Società corrompa 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).
- *Illecita influenza sull'assemblea (art. 2636 c.c.)*
  Nel caso in cui il Socio, con atti "simulati o fraudolenti", determini la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto.
- *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377- bis c.p.)*
  Nel caso in cui un esponente della Società offra o prometta somme di denaro ad un Socio per indurlo a non rendere dichiarazioni o rendere dichiarazioni mendaci all'autorità giudiziaria;
- *Ricettazione, riciclaggio e impiego di denaro, beni o altre utilità di provenienza illecita nonché autoriciclaggio*
  Nel caso di intromissione dei Soci nell'acquisto, nella ricezione o nell'occultamento di denaro o cose provenienti da un qualsiasi delitto.

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto di quanto indicato nel Codice Etico e dei seguenti **principi generali di comportamento:**

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle comunicazioni sociali, al fine di fornire al Socio ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- porre la massima attenzione ed accuratezza nell'acquisizione, custodia, elaborazione ed illustrazione dei dati e delle informazioni sociali;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento dell'Organizzazione e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà collegiale;
- assicurare l'espletamento delle proprie funzioni nel rispetto e nei limiti dei poteri formalmente ricevuti, nell'ambito delle proprie competenze, con obbligo di riporto al superiore gerarchico, anche conformandosi alle procedure adottate dalla Società;
- garantire la tracciabilità della trasmissione dei dati, anche mediante un Sistema informatico di gestione e controllo;
- assicurare il corretto svolgimento dei rapporti contrattuali intercorrenti con altre società.

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

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi e lacunosi o comunque non rispondenti alla realtà sulla situazione economica patrimoniale e finanziaria;
- omettere dati ed informazioni imposte dalla legge sulla situazione economica patrimoniale e finanziaria della Società;
- effettuare operazioni sugli utili non previste dalle leggi in vigore;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti (cartacei od informatici) o l'uso di altri mezzi fraudolenti o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Collegio Sindacale;
- porre in essere qualsiasi comportamento di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione da parte di Autorità pubbliche;
- compiere azioni o tentare comportamenti che possano anche solo essere interpretati quali pratiche di corruzione, favori illegittimi o che possano generare privilegi per sé e/o altri;
- effettuare spese di rappresentanza che prescindano dagli obiettivi della Società, non espressamente previste nel budget di periodo approvato ;
- ammettere compensi non correlati al tipo di incarico svolto sulla base del contratto sottoscritto;
- offrire doni e/o altre utilità al di fuori di quanto previsto dalla prassi aziendale e dalle procedure esistenti. In particolare, non devono essere offerti ai rappresentanti e/o ai dipendenti di società private e/o di enti ed organismi pubblici regali, doni, prestazioni gratuite di qualsivoglia genere - salvo quelle espressamente previste nei contratti o che occorrono alla promozione o alla diffusione delle iniziative e degli eventi di Teleconsys - che possano apparire connesse con il rapporto contrattuale con la Società o mirate a influenzare l'indipendenza di giudizio, o assicurare alla Società un qualsivoglia vantaggio;
- analogamente e reciprocamente, accettare doni e/o altre utilità al di fuori di quanto previsto dalla prassi aziendale e dalle procedure esistenti. Ove si realizzi, configurando un tentativo di corruzione da parte di amministratori, dirigenti, dipendenti o collaboratori di società private, non dovrà darsi seguito alla proposta e del fatto dovrà esser data pronta comunicazione al proprio diretto superiore o all'Organo amministrativo e, in ogni caso, all'OdV.

5.9.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Per l'attuazione delle regole elencate nel precedente paragrafo, devono essere rispettate le procedure specifiche di seguito descritte per le singole attività sensibili.

a) Gestione dei rapporti con i Soci, Collegio Sindacale e Società di revisione

- correttezza e trasparenza nei rapporti di natura commerciale con i Soci, 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;
- determinazione dei corrispettivi applicati alle operazioni commerciali e/o finanziarie

intercorse con i soci azionisti di Teleconsys secondo le "regole del mercato";

- 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;

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 ulteriori 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 dell'O.d.V con il Collegio Sindacale e la società di revisione.

b) Gestione degli adempimenti relativi al funzionamento degli organi societari

Nelle attività di gestione degli adempimenti societari e di segreteria societaria (calendarizzazione degli eventi societari, convocazioni, predisposizione documenti per il Consiglio di Amministrazione, verbalizzazione, archiviazione della documentazione, tenuta dei libri verbali), le prassi vigenti devono garantire il rispetto dei seguenti Protocolli specifici di comportamento e di controllo:

- le sedute del Consiglio di Amministrazione e dell'Assemblea dei Soci devono essere convocate con le modalità e entro i termini di legge, della normativa e della regolamentazione interna in materia;
- le attività di segreteria societaria finalizzate allo svolgimento delle sedute del Consiglio di Amministrazione e dell'Assemblea dei Soci devono garantire la predisposizione e la messa a disposizione della documentazione a supporto della discussione in tempi utili per poter garantire la corretta e puntuale informativa dei membri del Consiglio di Amministrazione e del Collegio sindacale e per consentire agli stessi la preventiva analisi, la successiva discussione in sede collegiale e l'assunzione di decisioni in modo informato e consapevole;
- le convocazioni con l'ordine del giorno, la documentazione propedeutica alla trattazione (della quale deve restare traccia, anche solo informatica, della provenienza dal competente Organo/Funzione) e le copie dei verbali e delle delibere, devono essere archiviati e conservati, in base alle rispettive competenze, presso la Segretaria anche solo con mezzi informatici;
- il Consiglio di Amministrazione ed il Collegio Sindacale nominano un segretario che cura la verbalizzazione delle rispettive riunioni; i verbali sono riportati in originale nei relativi libri e firmati dai presidenti e dai segretari.
- i membri del Consiglio di Amministrazione devono comunicare tempestivamente al Consiglio stesso ogni interesse che i medesimi, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata;
- il consigliere delegato che sia portatore di un interesse in una determinata operazione della società, ai sensi dell'art. 2391 c.c., deve astenersi dalla stessa, rimettendola alle determinazioni dell'intero consiglio;
- in entrambi i casi di cui ai due punti precedenti, la deliberazione del Consiglio di Amministrazione deve adeguatamente motivare le ragioni e la convenienza dell'operazione;
- consegna a tutti i componenti del Consiglio di Amministrazione e dell'Assemblea dei Soci, con adeguato anticipo e con documentata certificazione dell'avvenuta consegna, della bozza del progetto di Bilancio, prima della riunione per l'approvazione dello stesso;
- consegna unitamente a detta bozza delle relazioni accompagnatorie redatte dal Collegio sindacale, nonché delle attestazioni e relazioni del Dirigente preposto alla redazione dei documenti contabili societari.

c) Gestione delle operazioni societarie straordinarie (es. acquisizione di quote, di partecipazione in società del medesimo business)

- Le deliberazioni sulla destinazione di utili o riserve, nonché tutte le attività poste in essere nell'ambito di operazioni straordinarie sulle partecipazioni o sul capitale, devono rispettare lo Statuto e la normativa di riferimento;
- Devono essere seguite delle procedure autorizzative per l'assunzione di partecipazioni in altre società, consorzi e/o imprese, nonché per la valutazione, autorizzazione e gestione delle operazioni sul capitale (riduzione del capitale sociale, fusioni, scissioni);
- In particolare, le prassi vigenti devono garantire il rispetto dei seguenti protocolli specifici di

comportamento e di controllo:

- la decisione di effettuare un'operazione straordinaria deve essere condivisa dal soggetto delegato dal Consiglio di Amministrazione, dal Consiglio di Amministrazione o dall'Assemblea, in funzione della rilevanza della stessa (soglie definite dagli organi competenti/statuto) e dei limiti di legge;
- la gestione di operazioni straordinarie quali fusioni, acquisizione di partecipazioni rilevanti, cessione di partecipazioni in società controllate o scissioni, deve prevedere il coinvolgimento, per le parti di competenza, delle diverse Direzioni/Funzioni aziendali competenti ed, eventualmente, di consulenti esterni per lo svolgimento delle seguenti attività:
  a) analisi preliminare/due diligence di dati economici, finanziari e patrimoniali della / delle società interessate dall'operazione, nonché analisi di carattere legale/societaria;
  b) predisposizione della documentazione contrattuale;
  c) predisposizione di documentazione, bilanci e relazioni in merito alle operazioni straordinarie definite;
- in particolare devono essere verificate: la fattibilità finanziaria dell'operazione straordinaria, il rispetto della normativa vigente, il rispetto delle previsioni di legge che riguardano le società quotate;
- le verifiche svolte dalle funzioni competenti devono risultare documentate e tracciate;
- la documentazione contrattuale relativa alle operazioni straordinarie (acquisizioni, conferimenti, scissioni, ecc.) deve essere rivista e approvata, in base alle competenze, dagli organi delegati prima di portarla in approvazione agli organi preposti;
- le operazioni straordinarie sono approvate dal competente organo delegato, dal Consiglio di Amministrazione e/o dall'Assemblea dei soci; qualora la competenza sia del Consiglio di Amministrazione, sarà il competente organo delegato a sottoporre al Consiglio l'operazione per l'approvazione;
- lo stesso CdA può inoltre demandare ad un Amministratore, con specifica delibera comprensiva di apposita delega e nei limiti di legge e Statuto, il compimento dei successivi atti necessari alla conclusione dell'operazione;
- la documentazione fornita agli organi di volta in volta responsabili dell'approvazione deve essere adeguatamente conservata agli atti e il suo contenuto deve essere chiaro, veritiero ed esaustivo;
- la documentazione rilevante, copia delle convocazioni degli organi deputati all'approvazione dell'operazione, le relative delibere e i verbali devono essere archiviati e conservati presso la funzione competente;
- le operazioni straordinarie relative a società partecipate devono essere approvate anche dal Consiglio di Amministrazione ed eventualmente dall'Assemblea dei soci, in base alle competenze, della società interessata;
- le registrazioni contabili relative a operazioni a carattere straordinario (come per esempio fusioni, aumenti di capitale e destinazioni di utili o riserve) possono essere effettuate solo successivamente alla delibera favorevole da parte degli organi preposti e in coerenza con i termini di efficacia dell'operazione stessa;
- esame e parere consultivo dell'OdV su richiesta dell'Organo amministrativo su qualsiasi operazione di gestione straordinaria, od ordinaria che per valore o per tipologia risulti di particolare interesse o rischiosità per la Società.

d) Tutela dell'integrità di beni giuridici della Società

È fatto espresso divieto di:

- restituire conferimenti al Socio o liberarlo dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- ripartire riserve nei casi in cui ciò non sia consentito dalla legge;
- acquistare o sottoscrivere partecipazioni della Società, o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un ingiusto danno;
- procedere a formazione o ad aumenti fittizi del capitale sociale, attribuendo partecipazioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- porre in essere comportamenti che impediscano materialmente al Collegio Sindacale e all'Organismo di Vigilanza lo svolgimento delle loro rispettive attività di controllo e vigilanza, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti.

5.10. ACCORDI, PARTNERSHIP, RTI CON TERZE PARTI

5.10.1. 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:

- 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.

5.10.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività aziendali sulla base di accordi, convenzioni e partnership con terze parti (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 (art. 318, 319 c.p.)*

il reato potrebbe essere commesso 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

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

la fattispecie si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio induca un esponente del 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.

➢ *Corruzione ed istigazione alla corruzione tra privati (art. 2635-bis c.c.)*

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 (art. 416, escluso comma 6 c.p.)*

tale delitto è configurabile in tutti i casi in cui tre o più persone si associno allo scopo di commettere più delitti, tra quelli mappati nel presente Modello, rilevanti ai fini del D.lgs. 231/01, ovvero anche al fine di commettere reati che non siano ricompresi nel catalogo dei reati presupposto dal D.lgs. 231/01. Pertanto potrebbe essere commesso tra i diversi membri della partnership.

➢ *Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)*

➢ *Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)*

5.10.3. 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 responsabili della gestione dei rapporti con le controparti sono soggetti muniti di idonei poteri, distinguendo la fase d'instaurazione iniziale del rapporto dalle fasi di gestione;
- la scelta delle controparti dell'accordo/joint venture/partnership avviene dopo avere svolto idonee verifiche sulla reputazione (correttezza, trasparenza, competenza, professionalità) e sulla affidabilità sul mercato degli stessi, nonché dopo avere condiviso i fondamentali principi etici che guidano la Società. Devono essere svolte attente valutazioni di opportunità nel caso di controparti dal profilo soggettivo dubbio (in generale ogni indizio che possa far dubitare della "serietà professionale" della controparte) evitando, in questi casi, la definizione dell'accordo, joint venture e partnership;
- le diverse funzioni aziendali, per la propria area di competenza, sono coinvolte ai fini della valutazione dell'accordo/joint venture/partnership;
- è formalizzato il contratto che descrive le attività svolte per conto della controparte e disciplina le modalità e i principi con i quali sono gestiti i rapporti tra la Società e la stessa, in particolare per quanto concerne le condizioni economiche concordate;
- sono identificati gli strumenti più adeguati per garantire che i rapporti tenuti con la controparte siano sempre trasparenti, documentati e verificabili;
- sono autorizzati preventivamente l'utilizzo di dati e di informazioni destinati ad atti, comunicazioni, attestazioni e richieste di qualunque natura;
- sono sottoscritti con la controparte accordi di riservatezza (*non disclosure agreement*) a tutela delle Informazioni Confidenziali dell'Azienda;
- è verificato che la documentazione, le dichiarazioni e le informazioni trasmesse dalla Società siano complete e veritiere;
- è previsto un sistema di reporting verso il Vertice aziendale contente informazioni in merito alle controparti dell'accordo/joint venture/partnership, esito degli incontri, principali problematiche emerse, ecc.;
- nell'ambito degli 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;

- è conservata la documentazione relativa all'operazione in un apposito archivio, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

5.11. AREA LEGAL

5.11.1. 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:

- Contrattualistica
- Contenzioso e pre-contenzioso
- Audit

5.11.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività aziendali connesse all'area legale espone la Società, in via potenziale, alla commissione (anche in concorso) dei seguenti principali reati:

- *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)*
  Per es. mediante atti di violenza o minaccia nei confronti di una persona chiamata a rendere, davanti all'autorità giudiziaria, dichiarazioni utilizzabili in un procedimento giudiziario in cui è coinvolto l'Ente.
- *Corruzione in atti giudiziari (art. 319-ter c.p.) ed istigazione alla corruzione*
  Ad es. ponendo in essere un comportamento corruttivo nei confronti di un magistrato per favorire o danneggiare una parte in un processo civile, penale o amministrativo, in cambio del pagamento di una somma di denaro ovvero l'attribuzione di una consulenza a persona gradita al giudice.
- *Truffa ai danni dello Stato (art. 640 c. 2, n. 1 c.p.)*
  Falsificando o alterando il contenuto della documentazione destinata al magistrato, al CTU o ad un componente del collegio arbitrale.
- *Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)*
  Laddove 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 ed istigazione alla corruzione tra privati (art. 2635-bis c.c.)*
  Se un referente della Società dia o offra/prometta denaro o altra utilità non dovuta al legale o al Consulente Tecnico della controparte per ottenere un vantaggio per Teleconsys.

5.11.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto delle procedure aziendali che prevedono quanto segue:

Contrattualistica

- verifica correttezza e completezza dell'articolato contrattuale e coerenza con gli allegati predisposti dalle funzioni responsabili. Di tale attività di controllo viene lasciata traccia nello scambio di e-mail;
- nei contratti con clienti, fornitori, consulenti, partner e collaboratori vengono inserite specifiche clausole per il rispetto del Modello e del Codice Etico nonché apposita clausola che regoli le conseguenze della violazione delle norme e dei principi ivi contemplati (es. clausole risolutive espresse, penali con riserva di richiedere il risarcimento qualora dal comportamento tenuto derivino danni concreti alla Società).

Contenzioso e pre-contenzioso

La gestione di eventuali contenziosi ed accordi transattivi per prevenire o dirimere una controversia al fine di evitare l'instaurarsi o il proseguire di procedimenti giudiziari prevede l'accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio delle singole fasi del processo in capo alla Area legale, nel rispetto dei seguenti protocolli specifici di comportamento e di controllo:

- il processo può articolarsi nelle seguenti fasi: stragiudiziale o pre-contenziosa; contenziosa; gestione della pratica ed eventuale conferimento dell'incarico al legale esterno; controllo della prestazione e fatturazione da parte del legale esterno;
- il coinvolgimento di legali esterni deve essere concordato e coordinato dal responsabile dell'ufficio legale ed è formalizzato attraverso lettera d'incarico, contratto, mandato alle liti e ordine;
- deve essere garantita la tracciabilità, l'archiviazione e conservazione della documentazione relativa alla gestione dei contenziosi, con particolare riferimento a: i) motivi che hanno portato all'apertura del contenzioso; ii) criteri per cui è stato selezionato il legale e la definizione; iii) strategia da adottare nel contenzioso; iv) decisione di accettare/proporre eventuali transazioni;
- il responsabile dell'ufficio legale riferisce periodicamente al CdA e agli Organi di Controllo sull'attività stragiudiziale e sui contenziosi in essere e tempestivamente in occasione di fatti rilevanti.

Attività di auditing

- L'attività di auditing è specificamente regolamentata. E' definito un Piano di audit per la verifica della corretta applicazione del SGI integrato e la sua conformità agli standard ISO 9001 e ISO/IEC 27001 – 27017 – 27018 - 56002 e i servizi IT specifici dell'ambito 20000;
- al termine di ogni audit vengono formalizzati in un report le attività svolte ed i risultati ottenuti
- laddove vengano riscontrati disallineamenti tra gli aspetti operativi e le prescrizioni procedurali, essi sono formalizzati in rilievi, così classificati:
    - non conformità maggiori: Scostamenti con impatto significativo o diffusi sul SGI o sui servizi, incluse violazioni di aspetti di natura cogente;
    - non conformità minori: Scostamenti puntuali dall'applicazione delle procedure o con impatto minimo sul SGI;
    - opportunità di miglioramento: da prendere in considerazione per il miglioramento del SGI e dei suoi processi.

5.12. OMAGGI, SPONSORIZZAZIONI, INIZIATIVE PROMOZIONALI E MARKETING

5.12.1. ATTIVITÀ A RISCHIO

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

- concessione di omaggi, donazioni, liberalità, laddove superino i limiti e le modalità definiti nel Codice Etico e nei protocolli specifici di seguito riportati e laddove finalizzati all'acquisizione impropria di benefici in favore di funzionari pubblici, loro familiari e persone con le quali i funzionari intrattengono notoriamente stretti legami;
- sponsorizzazioni e erogazione di forme diverse di aiuti o contribuzioni, laddove abbiano la finalità di promuovere o favorire interessi della Società, a seguito di illecite pressioni;
- attribuzione di utilità aziendali a soggetti appartenenti alla Pubblica Amministrazione, laddove volta ad ottenere in cambio comportamenti illeciti favorevoli per la Società;
- partecipazione ad eventi, incontri di settore, laddove graditi a soggetti pubblici o a soggetti privati, a fronte del pagamento di un corrispettivo fuori mercato, per ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione amministrativa/contrattuale;
- riconoscimento di compensi ad agenzie per attività di promozione e di pubblicità, laddove finalizzati a costituire fondi da utilizzare a fini corruttivi;
- attività di marketing, laddove attuata con la finalità di influenzare indebitamente la decisione del potenziale Cliente;
- gestione dei social media, se utilizzati per denigrare un concorrente o i suoi prodotti/servizi (Pubblicità menzognera e/o denigratoria);
- rapporti con la stampa e con gli altri mezzi di comunicazione di massa.

5.12.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le eventuali iniziative della Società consistenti in omaggi, partecipazione ad eventi ed incontri di settore, sponsorizzazioni e marketing, costituiscono una modalità strumentale attraverso cui, in linea di principio, potrebbero essere commessi (anche in concorso) i seguenti principali reati:

- *Corruzione (art. 318, 319 c.p.)*
- *Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)*
  concedendo omaggi eccedenti i limiti del modico valore per ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione amministrativa/contrattuale
- *Corruzione in atti giudiziari (art. 319-ter c.p.)*
  con offerta o concessione di omaggi, donazioni, liberalità al fine di indurre qualcuno a non rendere dichiarazioni o a renderne di mendaci all'autorità giudiziaria
- *Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)*
  atti di concorrenza sleale ai sensi dell'art. 2598 c.c., quali Pubblicità menzognera o denigratoria, a mezzo stampa o social media per denigrare un competitor
- *Corruzione ed istigazione alla corruzione tra privati (art. 2635-bis c.c.)*
  sponsorizzazioni per ottenere in cambio vantaggi o altri trattamenti di favore

5.12.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre a quanto espresso nel Codice Etico, la Società, ai fini dell'attuazione delle regole e dei divieti relativi alla gestione di omaggi e altre forme di liberalità, sponsorizzazioni, eventi ed incontri di settore, attività di comunicazione e marketing, prevede le seguenti regole di condotta:

- chiara identificazione delle funzioni aziendali responsabili e coinvolte nella gestione degli omaggi;
- divieto di dare, offrire o promettere - anche indirettamente - denaro, doni, favori, beni, servizi o prestazioni non dovuti, in relazione a rapporti intrattenuti con pubblici ufficiali, incaricati di pubblico servizio, Enti pubblici o loro dipendenti;
- definizione e rispetto e tracciabilità dell'iter autorizzativo per l'attribuzione di omaggi;
- gli omaggi devono:
  - essere ragionevoli, di modico valore e comunque tali da non poter essere interpretati come finalizzati ad ottenere un trattamento di favore e da non compromettere l'integrità o la reputazione;
  - essere rivolti verso soggetti che svolgono ruoli inerenti le attività aziendali e che rispondono ai requisiti di reputazione e di onorabilità generalmente riconosciuti;
  - tenere conto del profilo del soggetto beneficiario, con riguardo alle consuetudini nei rapporti istituzionali o professionali;
  - essere documentati in modo adeguato per consentirne la tracciabilità, salvo per spese di valore esiguo;
  - essere effettuati dagli amministratori, dai dirigenti e dai dipendenti in funzione dell'attività svolta e del ruolo ricoperto all'interno della Società.
- adozione di sistemi di tracciabilità degli omaggi in uscita e dei relativi destinatari;
- elaborazione annuale un report di tutti gli omaggi in uscita;
- concessione di donazioni ed erogazioni liberali coerenti con i valori aziendali espressi nel Codice Etico;
- identificazione delle funzioni aziendali responsabili e coinvolte nella gestione delle donazioni ed erogazioni liberali;
- esistenza di segregazione tra chi approva il budget delle donazioni ed erogazioni liberali, chi le richiede e chi le autorizza;
- verifica sui beneficiari delle donazioni ed erogazioni liberali, finalizzata a verificare il tipo di organizzazione e la finalità per la quale è costituita e ad accertare che non vi siano condizioni di incompatibilità o conflitto di interessi, anche con riguardo ai rapporti di parentela o alle relazioni di carattere personale o professionale del destinatario;
- tutte le operazioni di donazioni ed erogazioni liberali devono essere approvate dai soggetti dotati di idonei poteri in base al sistema dei poteri e delle deleghe;
- elaborazione annuale di un report di tutti le donazioni ed erogazioni liberali effettuate da parte della Funzione responsabile;
- archiviazione della documentazione prodotta in relazione alle donazioni ed erogazioni liberali, anche al fine di garantire la tracciabilità del processo.

- gli eventi di marketing devono essere orientati a rappresentare in modo corretto e veritiero 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;
- 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.

5.13. RAPPORTI NON COMMERCIALI CON LA PUBBLICA AMMINISTRAZIONE

5.13.1. 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 in cui svolgano attività di Pubblico Ufficiale.

5.13.2. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

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 (art. 318, 319 c.p.)*
  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;
- *Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)*
  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;
- *Truffa in danno dello Stato, di altri enti pubblici o delle Comunità europee (art. 640 c. 2, n. 1 c.p.)*
  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;
- *Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)*
  nel caso in cui gli artifici o raggiri si sostanzino nella comunicazione di dati non veri o nella predisposizione di una documentazione falsa, per ottenere finanziamenti pubblici o erogazioni pubbliche;

- *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)*
  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.

Nell'ambito delle fattispecie di reati sopra indicate:

- "Pubblici Ufficiali": sono coloro che, pubblici dipendenti o privati, possano o debbano formare e manifestare la volontà della pubblica amministrazione, ovvero esercitare poteri autoritativi o certificativi, nell'ambito di una potestà di diritto pubblico (art. 357 c.p.).
- "Incaricati Di Pubblico Servizio": sono coloro i quali, a qualunque titolo, prestano un pubblico servizio, senza essere dotati dei poteri tipici della pubblica funzione, quali quelli autoritativi e certificativi. (art. 358 c.p.).

A titolo esemplificativo e non esaustivo:

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.).

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").

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);

6. RISK ASSESSMENT

Il processo di analisi dei rischi è fondamentale per realizzare un efficiente ed efficace Modello di organizzazione e per tenerlo costantemente aggiornato.
La modalità di valutazione utilizzata ha analizzano i rischi per ogni singola area aziendale sensibile (area commerciale, finanziaria, acquisti, ecc…) in relazione alle singole fattispecie di reato potenzialmente

interessanti tale area.
Secondo gli indici di **probabilità** e **impatto**, è stata calcolata l'entità del rischio che determina l'applicazione di eventuali azioni preventive e correttive.

- La **PROBABILITÀ** esprime il numero di volte che l'evento dannoso può verificarsi ed è stata stimata dal Responsabile della Funzione/Area interessata, secondo i seguenti fattori di valutazione (range da 0 a 100):
  - Potenziale vantaggio/opportunità ottenibile con il reato (da 0 a 40)
  - Assenza o inefficacia di controlli (da 0 a 30)
  - Frequenza dell'attività sensibile (da 0 a 30)

Con il seguente Rating di probabilità:

PROBABILITA' **P**
per un punteggio > 90
per un punteggio tra 65-90
per un punteggio tra 40-64
per un punteggio tra 20-39
per un punteggio < 20

VALORE
Elevata (5)
Alta (4)
Moderata (3)
Bassa (2)
Nulla (1)

- L'**IMPATTO** è la quantificazione dell'evento dannoso, laddove questo si verificasse ed è stimata in base alle sanzioni (interdittive e pecuniarie) applicabili per la singola fattispecie di reato, come segue:

I (Impatto)
CRITICO oltre 700 quote
ALTO fino 700 quote
MODERATO fino 330 quote
BASSO fino 100 quote

La determinazione dell'esposizione al **RISCHIO**, per ciascun articolo del D.Lgs. 231 (e in riferimento all'articolo di codice civile o penale), è data da probabilità x impatto (**R = P x I)**

RISCHIO = **PROBABILITÀ** x **IMPATTO**

Probabilità				
5 elevata	10	15	20	25
4 alta	8	12	16	20
3 moderata	6	9	12	15
2 bassa	4	6	8	10
	2 basso	3 moderato	4 alto	5 critico
	Impatto			

Al termine dell'analisi, a seconda del livello di rischio calcolato, le azioni preventive e correttive per prevenire, eliminare o ridurre le cause dei possibili rischi dovranno essere adottate nei termini indicati come segue:

RISCHIO	AZIONI NECESSARIE
≥ 20 CRITICO	entro 1 settimana
< 20 ALTO	entro 1 mese
< 15 MODERATO	entro 1 anno
< 10 BASSO	nessuna azione

In allegato al presente modello, le schede di RISK ASSESMENT per le seguenti aree aziendali a rischio:

1. ATTIVITÀ COMMERCIALI E DI VENDITA DEI PRODOTTI E SERVIZI
2. GESTIONE DEGLI ACQUISTI DI BENI E SERVIZI DA TERZI
3. REALIZZAZIONE COMMESSE, "DELIVERY" E SERVIZI
4. SISTEMI INFORMATIVI AZIENDALI
5. GESTIONE DEL PERSONALE
6. AMMINISTRAZIONE, FINANZA, CONTROLLO

7. SALUTE E SICUREZZA NEI LUOGHI DI LAVORO
8. AMBIENTE
9. RAPPORTI CON I SOCI, COLLEGIO SINDACALE E SOCIETÀ DI REVISIONE
10. ACCORDI, PARTNERSHIP, RTI
11. AREA LEGALE
12. INIZIATIVE PROMOZIONALI E MARKETING
13. RAPPORTI NON COMMERCIALI CON LA PUBBLICA AMMINISTRAZIONE