CENTRO DIAGNOSTICO RADIOLOGICO CAMPIONE S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D.Lgs. 8 giugno 2001, n. 231

CODICE DI CONDOTTA

Rev. 00 – Luglio 2026

INDICE

1. PREMESSA

Il presente documento contiene le "Linee di Condotta" alle quali Amministratori, Sindaci, dirigenti, dipendenti della Società e in generale tutti coloro che operano in nome e/o per conto e/o nell'interesse della Società, o che con la stessa intrattengono relazioni di affari ("Destinatari delle Linee di Condotta") devono attenersi per evitare il determinarsi di situazioni ambientali favorevoli alla commissione di fatti illeciti in genere, e tra questi in particolare dei reati rilevanti ai sensi del d.lgs. 231/20011.
Le Linee di Condotta individuano, se pur a titolo non esaustivo, comportamenti relativi all'area del "fare" e del "non fare", con riferimento in particolare ai rapporti con la Pubblica Amministrazione (o anche "PA"), con i soggetti terzi, nonché alle attività e agli adempimenti societari, al corretto utilizzo degli strumenti informatici ed ai rapporti con i dipendenti, specificando in chiave operativa quanto espresso dai principi del Codice Etico.
I Destinatari delle Linee di Condotta sono impegnati al rispetto delle leggi e dei regolamenti vigenti nel paese in cui la Società opera.
I Destinatari delle Linee di Condotta sono impegnati al rispetto delle procedure aziendali e si ispirano ai principi del Codice Etico in ogni decisione o azione attinente alla gestione della Società.
I Responsabili di funzione o Responsabili Interni devono curare che:

- per quanto ragionevolmente possibile, tutti i dipendenti siano edotti sulla normativa e sui comportamenti conseguenti e, qualora abbiano dei dubbi sulle modalità da seguire, siano adeguatamente indirizzati;
- sia attuato un adeguato programma di formazione e sensibilizzazione continua sulle problematiche attinenti al Codice Etico.

2. PRINCIPI DI COMPORTAMENTO NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Di seguito vengono esposti i principi di comportamento relativi all'area del "fare" e del "non fare", specificando in chiave operativa quanto espresso dai principi del Codice etico, da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex D. Lgs. 231/01 ed in particolare da quanto previsto dall'art.24 del dlgs 231/01.

Area del "fare"

I responsabili delle funzioni che hanno contatti formali ed informali con la Pubblica Amministrazione devono:

- dare ai propri collaboratori indicazioni precise sulle modalità di comportamento da assumere con i diversi soggetti pubblici, infondendo la conoscenza della norma nonché la consapevolezza delle circostanze che possono essere a rischio reato;
- prevedere da e verso la Pubblica Amministrazione sistemi di tracciabilità dei flussi informativi;
- prevedere una apposita clausola di stretta osservanza dei principi etici adottati dalla Società nel caso di incarichi attribuiti a soggetti esterni che operano in qualità di rappresentanti dell'Ente; inoltre tali incarichi devono essere conferiti in maniera formale;
- prevedere che dipendenti e collaboratori esterni si impegnino a comunicare all'Organismo di Vigilanza, unicamente in forma non anonima, qualsiasi violazione o sospetto di violazione del Modello Organizzativo.

Di converso, l'Ente e l'Organismo di Vigilanza dovranno salvaguardare i dipendenti e i collaboratori esterni da qualsivoglia effetto pregiudizievole che possa discendere dalla segnalazione.
L'Organismo di Vigilanza allo stesso modo tutela la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.

Area del "non fare"

Nei rapporti con i rappresentanti della Pubblica Amministrazione è vietato:

- promettere o effettuare erogazioni in denaro aventi ad oggetto fini diversi da quelle istituzionali e di servizio;
- effettuare spese di rappresentanza senza giustificativi e aventi scopi diversi da obiettivi prettamente aziendali;
- promettere o concedere direttamente o indirettamente omaggi/regalie dirette o indirette di ingente valore;
- procurare o promettere di procurare informazioni e/o documenti riservati;
- favorire, nei processi d'acquisto, fornitori e sub-fornitori segnalati dai rappresentanti stessi della Pubblica Amministrazione come condicio sine qua non per il futuro svolgimento delle attività (es. affidamento della commessa, concessione del finanziamento agevolato).

I divieti di cui sopra devono ritenersi altresì validi nei rapporti indiretti con i rappresentanti della Pubblica Amministrazione mediante terzi fiduciari.
Inoltre, nei confronti della Pubblica Amministrazione, è vietato:

- esibire documenti falsi o artefatti;

- assumere un comportamento menzognero al fine di indurre in errore la Pubblica Amministrazione;
- nella valutazione tecnico-economica riguardante i servizi offerti/forniti, tralasciare volutamente informazioni dovute, al fine di rivolgere a proprio favore le decisioni della Pubblica Amministrazione;
- destinare contributi/sovvenzioni/finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti;
- accedere, senza autorizzazione, ai sistemi informativi della Pubblica Amministrazione, al fine di procurarsi e/o modificare informazioni a vantaggio dell'Azienda;
- abusare della posizione di incaricato di pubblico servizio per ottenere utilità a vantaggio dell'Azienda.

3. PRINCIPI DI COMPORTAMENTO PER LE ATTIVITA' RELATIVE ALLE COMUNICAZIONI SOCIALI

Di seguito vengono esposti i principi di comportamento da seguire per evitare di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato previste dall'art. 25 ter del D.Lgs. n. 231/01 e dall'art. 25 ter – comma 1 (introdotto dal D.L. 190/2012).

Area del "fare":

I soggetti e i servizi coinvolti nelle attività relative alle comunicazioni sociali devono:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali;
- osservare tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, ed agire sempre nel rispetto delle procedure interne aziendali, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento dell'Ente e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge.

Area del "non fare":

Si evidenziano qui di seguito le condotte che i soggetti su citati non devono porre in essere:

- rappresentare o trasmettere dei dati falsi, o comunque non rispondenti alla realtà, per l'elaborazione e la predisposizione di bilanci, relazioni e prospetti o altre comunicazioni sociali, sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- impedire materialmente le attività di controllo o comportamenti che risultino di ostacolo a tale attività;
- esporre, nelle predette comunicazioni e trasmissioni, fatti non rispondenti al vero, o occultare fatti rilevanti, relativamente alla situazione economica, patrimoniale e finanziaria dell'Ente.

4. PRINCIPI DI COMPORTAMENTO NEI RAPPORTI CON SOGGETTI INTERNI E TERZI ALLA SOCIETA'

Di seguito vengono esposte le linee guida di comportamento da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex D.Lgs. 231/01ed in particolare da quanto previsto dagli artt. 24 ter, 25 e 25 quater.

Area del "fare"

I soggetti e i servizi coinvolti nelle attività relative alla gestione della società e i soggetti che hanno potere di spesa devono:

- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nell'espletamento di tutte le attività svolte nell'ambito della Gestione dei rapporti con interlocutori terzi - pubblici o privati nello svolgimento delle proprie attività lavorative per conto e/o nell'interesse della Società;
- osservare tutti i regolamenti, i protocolli e le procedure che disciplinano l'attività aziendale, con riferimento all'approvvigionamento di beni, servizi e lavori, nonché con riferimento alle modalità di gestione delle risorse finanziarie;
- effettuare nel momento in cui si instaurano rapporti commerciali, siano essi di natura attiva o passiva, tutte le verifiche richieste da regolamenti, protocolli e procedure che disciplinano l'attività aziendale, o che appaiano comunque opportune in ragione delle caratteristiche soggettive del soggetto terzo con cui la Società viene in contatto e delle caratteristiche oggettive della prestazione oggetto del rapporto negoziale;
- i fornitori devono essere scelti con metodi trasparenti e secondo la specifica procedura;
- nei contratti con clienti e fornitori deve essere contenuta un'apposita clausola che regoli le conseguenze in caso di commissione di fatti rilevanti ai sensi del Decreto (es. clausola risolutiva espressa):
- effettuare un costante monitoraggio dei flussi finanziari aziendali;
- prevedere che dipendenti e collaboratori esterni si impegnano a comunicare all'Organismo di Vigilanza, unicamente in forma non anonima, qualsiasi violazione o sospetto di violazione del Modello Organizzativo.

Di converso, l'Ente e l'Organismo di Vigilanza dovranno salvaguardare i dipendenti e i collaboratori esterni da qualsivoglia effetto pregiudizievole che possa discendere dalla segnalazione.

L'Organismo di Vigilanza allo stesso modo tutela la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.

Nel caso in cui i responsabili di funzione vengano a conoscenza, in via diretta o indiretta, di comportamenti a rischio reato ex D.lgs 231/01 in merito ai processi operativi di competenza, o altresì di notizie, anche derivanti da organi di polizia giudiziaria, riguardanti illeciti e/o reati con rischi di impatto aziendale, sono tenuti a darne formale immediata comunicazione all'Organismo di Vigilanza.

Area del "non fare"

Nell'espletamento delle attività considerate a rischio, agli Esponenti Aziendali, in via diretta, e ai Consulenti e i Partner,in relazione al tipo di rapporto con la Società, è vietato:

- effettuare spese di rappresentanza senza giustificativi e aventi scopi diversi da obiettivi prettamente aziendali;

- procurare o promettere di procurare informazioni e/o documenti riservati;
- effettuare o ricevere pagamenti in contanti, salvo che si tratti di somme di modico valore, o di acquisti urgenti, che non possano essere preventivati;
- acquistare beni o servizi verso un corrispettivo palesemente inferiore al valore di mercato di tali beni o servizi, senza avere prima effettuato le necessarie verifiche sulla provenienza;
- instaurare e/o intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti.
- ostacolare lo svolgimento di eventuali indagini e iniziative da parte degli Organi sociali, o più in generale da qualsiasi organo/ente ispettivo, finalizzate a rilevare e combattere condotte illecite in relazione all'ipotesi del reato associativo considerato;
- promuovere, costituire, organizzare ovvero partecipare ad associazioni di tre o più soggetti con lo scopo di commettere uno o più delitti o, più in generale, tenere condotte direttamente o indirettamente vietate dalla legge penale;
- implementare e svolgere qualsivoglia iniziativa economica che, nella forma associativa e con le modalità di cui sopra, si ponga in contrasto con l'utilità sociale, recando danno alla sicurezza e alla libertà altrui, con conseguente violazione dell'ordine economico e dell'ordine pubblico;
- attuare - anche strumentalizzando attività riconducibili alla comune gestione societaria - condotte che si concretino in un'attiva e stabile partecipazione all'associazione illecita;
- contribuire - anche attraverso il proprio assetto organizzativo - a creare e garantire nel tempo una struttura organizzativa che, seppur minima, sia comunque idonea ed adeguata alla realizzazione di obiettivi delittuosi nell'interesse dell'associazione illecita;
- predisporre - ovvero contribuire a predisporre - i mezzi attraverso i quali supportare l'operatività della associazione illecita;
- promuovere o comunque proporre, la realizzazione di obiettivi delittuosi di volta in volta individuati come utili o necessari nell'ottica del conseguimento di un vantaggio per la Società.

5. PRINCIPI DI COMPORTAMENTO NEI RAPPORTI CON I DIPENDENTI

Di seguito vengono esposte le linee guida di comportamento da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex D.Lgs. 231/01ed in particolare da quanto previsto dagli artt. 25 septies e 25 doudecies.

Area del "fare"

I soggetti e i servizi coinvolti nelle attività a rischio devono:

- considerare sempre prevalente la tutela dei lavoratori rispetto a qualsiasi considerazione economica;
- verificare al momento dell'assunzione e durante lo svolgimento di tutto il rapporto lavorativo che eventuali lavoratori provenienti da paesi terzi siano in regola con il permesso di soggiorno e, in caso di scadenza dello stesso, abbiano provveduto a rinnovarlo;

- nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, assicurarsi che tali soggetti si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
- assicurarsi con apposite clausole contrattuali che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
- devono essere rispettate le misure previste dalle procedure aziendali dirette alla prevenzione dell'impiego del lavoro irregolare ed alla tutela dei lavoratori.
- prevedere che dipendenti e collaboratori esterni si impegnano a comunicare all'Organismo di Vigilanza, unicamente in forma non anonima, qualsiasi violazione o sospetto di violazione del Modello Organizzativo.

Di converso, l'Ente e l'Organismo di Vigilanza dovranno salvaguardare i dipendenti e i collaboratori esterni da qualsivoglia effetto pregiudizievole che possa discendere dalla segnalazione.
L'Organismo di Vigilanza allo stesso modo tutela la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.
Nel caso in cui i responsabili di funzione vengano a conoscenza, in via diretta o indiretta, di comportamenti a rischio reato ex D.lgs 231/01 in merito ai processi operativi di competenza, o altresì di notizie, anche derivanti da organi di polizia giudiziaria, riguardanti illeciti e/o reati con rischi di impatto aziendale, sono tenuti a darne formale immediata comunicazione all'Organismo di Vigilanza.

Area del "non fare"
Nell'espletamento delle attività considerate a rischio, agli Esponenti Aziendali, in via diretta, e ai Consulenti e i Partner, in relazione al tipo di rapporto con la Società, è vietato:

- fare ricorso, in alcun modo, al lavoro minorile o non collaborare con soggetti che vi facciano ricorso;
- fare ricorso, in alcun modo, all'impiego di immigrati irregolari.

6. PRINCIPI DI COMPORTAMENTO NELL'UTILIZZO DEGLI STRUMENTI INFORMATICI

Di seguito vengono esposte le linee guida di comportamento da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex D. Lgs. 231/01ed in particolare da quanto previsto dagli artt. 24 bis e 25 bis 1.

Area del "fare"
Tutti coloro che sono tenuti a conoscere il Documento Programmatico per la Sicurezza (DPS) in ragione del loro ufficio (i Responsabili, ed Incaricati del trattamento di dati, oltre a tutti coloro che di fatto trattino dati soggetti alle disposizioni dell'art. 34 D. Lgs. 196/2003), dovranno uniformare i loro comportamenti e le loro azioni alle disposizioni ivi contenute.
Le misure generali per la prevenzione dei reati informatici, e poste a presidio di attività finalizzate al trattamento illecito di dati, sono:

- la previsione di idonee procedure per l'assegnazione e la gestione di credenziali di autorizzazione personali (*username, password e smart card*) e la determinazione di coerenti termini di validità delle medesime;

- la previsione di idonee procedure per l'autenticazione ed il conseguente accesso agli strumenti informatici;
- il conferimento a Dirigenti, Dipendenti, Consulenti e Partners delle credenziali di accesso alle diverse sezioni del sistema informatico aziendale, ed in genere a dati, informazioni, sistemi informatici e telematici cui la Società abbia accesso, nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico, e coerente agli obiettivi aziendali;
- la responsabilizzazione di ogni singolo utente riguardo le attività di salvataggio e memorizzazione di dati, nell'ambito dei più ampi presidi posti dalla Società a tutela della sicurezza, della integrità, e della riservatezza dei dati;
- il corretto utilizzo della posta elettronica aziendale per ragioni (di norma) giustificate da esigenze di servizio;
- prevedere che dipendenti e collaboratori esterni si impegnano a comunicare all'Organismo di Vigilanza, unicamente in forma non anonima, qualsiasi violazione o sospetto di violazione del Modello Organizzativo.

Di converso, l'Ente e l'Organismo di Vigilanza dovranno salvaguardare i dipendenti e i collaboratori esterni da qualsivoglia effetto pregiudizievole che possa discendere dalla segnalazione. L'Organismo di Vigilanza allo stesso modo tutela la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.

Area del "non fare"

Nell'espletamento delle attività considerate a rischio, agli Esponenti Aziendali, in via diretta, e ai Consulenti e i Partner, in relazione al tipo di rapporto con la Società, è vietato:

- modificare le configurazioni standard di software ed hardware aziendale;
- aggirare le regole di sicurezza imposte sugli strumenti informatici aziendali e sulle reti di collegamento interne ed esterne;
- eludere sistemi di controllo posti a presidio di, o al fine di restringere l'accesso a, sistemi informatici o telematici, e comunque di accedere ai predetti sistemi in mancanza delle necessarie autorizzazioni;
- trasmettere o comunicare a terzi, o di acquisire a qualsiasi titolo da terzi, password, codici, dati o informazioni di sorta, atti a consentire al solo legittimo detentore l'accesso o la permanenza all'interno di sistemi informatici o telematici;
- trasmettere attraverso lo strumento informatico di materiale di proprietà della Società e/o confidenziale qualora i destinatari siano indirizzi non definiti e riconosciuti dal sistema aziendale;
- trasmettere mail contenenti credenziali di autorizzazione personali (username e password, PIN e PUK della smart card) ovvero l'indirizzo di posta elettronica personale, in caso di comunicazioni al di fuori della realtà aziendale non motivate da ragioni di servizio;
- trasmettere comunicazioni comunque contrarie alla morale e dal buon costume;
- connettersi, navigare, consultare siti web che siano da considerarsi illeciti alla luce delle disposizioni organizzative interne e quindi, a titolo esemplificativo, siti che presentino contenuti:
  - ✓ contrari alla morale, alla libertà di culto ed all'ordine pubblico,
  - ✓ che consentano violazione della privacy di persone fisiche e giuridiche,

✓ che promuovano o appoggino movimenti terroristici o sovversivi, riconducibili ad attività di pirateria informatica,

✓ che violino le norme dettate in materia di copyright e di proprietà intellettuale

- modificare le configurazioni standard di software ed hardware aziendale;
- aggirare le regole di sicurezza imposte sugli strumenti informatici aziendali e sulle reti di collegamento interne ed esterne;
- eludere sistemi di controllo posti a presidio di, o al fine di restringere l'accesso a, sistemi informatici o telematici, e comunque di accedere ai predetti sistemi in mancanza delle necessarie autorizzazioni;
- trasmettere o comunicare a terzi, o di acquisire a qualsiasi titolo da terzi, password, codici, dati o informazioni di sorta, atti a consentire al solo legittimo detentore l'accesso o la permanenza all'interno di sistemi informatici o telematici;
- il personale dipendente non può divulgare attraverso i social media informazioni riservate, come la corrispondenza interna, informazioni di terze parti di cui è a conoscenza (ad esempio partner, istituzioni, utenti, stakeholder, ecc.) o informazioni su attività lavorative. Servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati, pubblicato e/o comunicati formalmente alle parti interessate;
- fermo restando il corretto esercizio delle libertà sindacali e del diritto di critica, il personale dipendente è tenuto ad astenersi dalla trasmissione e diffusione di messaggi minatori o ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti della Società, riferiti alle attività istituzionali dell'ente e più in generale al suo operato, che per le forme e i contenuti possano comunque nuocere alla Società, ledendone l'immagine o compromettendone l'efficienza;
- deve rispettare la privacy dei colleghi, evitando riferimenti all'attività lavorativa svolta, fatte salve le informazioni di dominio pubblico;
- non può divulgare foto, video, o altro materiale multimediale, che riprenda locali e personale senza l'esplicita autorizzazione dei vertici della società e degli uffici preposti
- non può aprire blog, pagine o altri canali recanti il nome o il logo o l'immagine della società che trattino argomenti riferiti all'attività istituzionale dell'ente, senza autorizzazione preventiva dei vertici societari e degli uffici preposti;
- non può utilizzare il logo o l'immagine della società in account personali e non lavorativi.

La violazione di tali regole di comportamento è fonte di responsabilità disciplinare, accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni.

6.1 Linee di condotta in materia di utilizzo di sistemi di intelligenza artificiale e protezione dei dati

Le funzioni aziendali, i dipendenti e i collaboratori sono tenuti a utilizzare i sistemi di intelligenza artificiale nel rispetto delle seguenti linee di condotta:

- l'impiego di sistemi di AI è consentito esclusivamente per finalità lecite, coerenti con le attività aziendali e previamente autorizzate secondo le procedure interne;
- è vietato utilizzare sistemi di AI in modo tale da aggirare o compromettere le misure di sicurezza informatica, i controlli di accesso o i presìdi di protezione dei dati personali;

- il trattamento di dati personali mediante sistemi di AI deve avvenire nel rispetto dei principi di necessità, proporzionalità e minimizzazione, nonché delle istruzioni organizzative e tecniche impartite dall'ente;
- i sistemi di AI devono essere utilizzati sotto adeguata supervisione umana, nel rispetto dei ruoli e delle responsabilità assegnate, evitando automatismi decisionali non autorizzati;
- eventuali anomalie, incidenti di sicurezza, utilizzi impropri o rischi di trattamento illecito dei dati devono essere tempestivamente segnalati secondo i canali previsti dal Modello 231 e dal sistema di gestione della sicurezza delle informazioni.

7. PRINCIPI DI COMPORTAMENTO IN MATERIA DI RISPETTO DELLE NORME DI TUTELA AMBIENTALE

Di seguito vengono esposte le linee guida di comportamento da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex D.Lgs. 231/01ed in particolare da quanto previsto dall'art.25 undecies.

Area del "fare"

I soggetti e i servizi coinvolti nelle attività relative al rispetto delle norme di tutela ambientale devono:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla tutela ambientale;
- conservare e compilare tutta la documentazione prescritta dalle norme di legge o dalle autorizzazioni amministrative;
- verificare e conservare tutte le autorizzazioni ambientali di soggetti terzi con cui la società intrattiene rapporti di collaborazione per attività che possano avere impatto sull'ambiente ovvero sono sottoposte alla disciplina del Testo unico ambientale;
- collaborare efficacemente con le autorità preposte ai controlli;
- riesaminare periodicamente i processi produttivi e le attività svolte con il fine di minimizzare gli impatti ambientali.

Area del "non fare"

Nell'espletamento delle attività considerate a rischio, agli Esponenti Aziendali, in via diretta, e ai Consulenti e i Partner, in relazione al tipo di rapporto con la Società, è vietato:

- eludere le procedure ed i sistemi di controllo interno in materia di rispetto della tutela ambientale;
- ostacolare le attività di controllo degli enti preposti alla verifica delle norme di tutela ambientale.

8. OBBLIGHI DI SEGNALAZIONE

I Destinatari delle Linee di Condotta hanno l'obbligo di segnalare all'Organismo di Vigilanza:

- ogni violazione o sospetta violazione delle Linee di Condotta e del Modello Organizzativo.

Le segnalazioni devono essere fornite in forma non anonima. A tal proposito la Società e l'Organismo di Vigilanza tutelano dipendenti e collaboratori terzi da eventuali conseguenze pregiudizievoli derivanti dalla segnalazione, assicurando la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.

A titolo esemplificativo, i responsabili interni provvedono a segnalare all'Organismo di Vigilanza:

- ✓ comportamenti a rischio reati ex d.lgs. 231/2001, relativi ai processi operativi di competenza di cui siano venuti a conoscenza in qualunque modo, anche attraverso collaboratori;
- ✓ provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, di cui si venga ufficialmente a conoscenza, riguardanti illeciti e/o ipotesi di reato di cui al d.lgs. 231/2001 con rischi di impatto aziendale.

9. SANZIONI

I comportamenti non conformi alle disposizioni delle presenti Linee di Condotta, comporteranno, indipendentemente ed oltre gli eventuali procedimenti penali a carico del/gli autore/i della violazione, l'applicazione di sanzioni individuate nel Codice Sanzionatorio e previste ai sensi della vigente normativa e/o contrattazione collettiva.