MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

DI

TEAMSYSTEM S.P.A.

AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

"*Responsabilità amministrativa della Società*"

Revisione	**Data**	**Approvazione**
00	16/03/2017	CdA
01	22/06/2017	CdA
02	15/07/2019	CdA
03	15/03/2021	CdA
04	27/07/2023	CdA

Indice

1 Definizioni

Decreto: il Decreto Legislativo 8 giugno 2001, n. 231[1].

Dipendenti: persone sottoposte alla direzione od alla vigilanza di uno dei soggetti apicali; quindi, ma non solo, tutti i soggetti, compresi i dirigenti, che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società nonché i lavoratori in distacco o in forza con contratti di lavoro parasubordinato.

Documento informatico: qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati a rielaborarli.

Illeciti amministrativi: gli illeciti amministrativi di cui all'art. 187-quinquies del Testo Unico delle disposizioni in materia di intermediazione finanziaria (T.U.F.).

Linee Guida di Confindustria: le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001 approvate da Confindustria in data 7 marzo 2002 (aggiornate a marzo 2014).

Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001: il presente Modello di organizzazione, gestione e controllo così come previsto *ex* D.Lgs. 231/2001.

Organismo di Vigilanza (OdV): l'Organismo di vigilanza previsto dal D.Lgs. 231/2001.

Reati: i reati di cui al Decreto legislativo 8 giugno 2001 n. 231.

Società: TeamSystem S.p.A..

Soggetti apicali: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione od il controllo della Società.

[1] E successive integrazioni e modificazioni: tale precisazione vale per qualsivoglia legge, regolamento o complesso normativo, che siano richiamati nel Modello.

2 Premessa

Il presente documento contiene la descrizione dei contenuti del Modello di Organizzazione, Gestione e Controllo ("Modello Organizzativo" o semplicemente "Modello") adottato da TeamSystem S.p.A. ("TeamSystem" o la "Società") ai sensi del D.lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni ("D.lgs. 231/2001" o "Decreto"), recante la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica.

TeamSystem ha adottato il Modello Organizzativo in data 16 marzo 2017 e lo ha successivamente aggiornato da ultimo con delibera del Consiglio di Amministrazione del 15 marzo 2021, nell'ambito delle proprie politiche di costante revisione, miglioramento e aggiornamento del proprio sistema di controllo per la prevenzione dei reati ai sensi del Decreto.

Il presente documento contiene le linee guida ed i principi generali di adozione descrittivi del Modello e si compone di una "Parte Generale", nonché della "Parte Speciale" e dei relativi allegati.

La Parte Generale contiene una sintetica illustrazione del Decreto e dei suoi contenuti, oltre alle regole ed i principi generali del Modello, l'identificazione dell'Organismo di Vigilanza e la definizione dei compiti, poteri e funzioni di tale organismo, la descrizione del sistema sanzionatorio e disciplinare; la definizione di un sistema di comunicazione, informazione e formazione sul Modello, nonché la previsione di verifiche periodiche e dell'aggiornamento del Modello.

La Parte Speciale contiene l'individuazione delle aree ed attività ritenute rilevanti per la Società, nonché la descrizione dei protocolli di controllo preventivi adottati in merito a ciascuna categoria di reato ritenuta rilevante per la Società ai sensi del D.lgs. 231/2001.

3 Il Decreto Legislativo 231/2001

I. La Responsabilità Amministrativa degli Enti

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto Legislativo n. 231 (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia ha già da tempo aderito, ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Con tale Decreto, dal titolo "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", è stato introdotto nell'ordinamento italiano un regime di responsabilità amministrativa a carico di enti (società, associazioni, ecc. di seguito denominati "Enti") per alcuni reati commessi, nell'interesse o vantaggio degli stessi da:

- persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa, 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 natura di questa nuova forma di responsabilità degli enti è di genere "misto" e la sua peculiarità risiede nel fatto che la stessa coniuga aspetti del sistema sanzionatorio penale e di quello amministrativo. In base al Decreto, infatti l'ente è punito con una sanzione di natura amministrativa, in quanto risponde di un illecito amministrativo, ma il sistema sanzionatorio è fondato sul processo penale: l'Autorità competente a contestare l'illecito è il Pubblico Ministero, ed è il giudice penale che irroga la sanzione.

La responsabilità amministrativa degli Enti si aggiunge a quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'Ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o non risulti punibile.

Il campo di applicazione del Decreto è molto ampio e riguarda tutti gli enti forniti di personalità giuridica, le società, le associazioni anche prive di personalità giuridica, gli enti pubblici economici, gli enti privati concessionari di un pubblico servizio. La normativa non è invece applicabile allo Stato, agli enti pubblici territoriali, agli enti pubblici non economici, e agli enti che svolgono funzioni di rilievo costituzionale (per esempio i partiti politici e i sindacati).

La norma non fa riferimento agli enti non aventi sede in Italia. Tuttavia, a tal proposito, un'ordinanza del Giudice per le Indagini Preliminari del Tribunale di Milano (ordinanza 13 giugno 2007; v. anche GIP Milano, ord. 27 aprile 2004, e Tribunale di Milano, ordinanza 28 ottobre 2004) ha sancito, in base al principio di territorialità, la sussistenza della giurisdizione del giudice italiano in relazione a reati commessi da Enti esteri in Italia.

II. I reati previsti dal Decreto

I reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell'Ente, sono quelli espressamente e tassativamente richiamati dal Decreto e successive modifiche ed integrazioni.

All'interno del presente documento, sono elencati tutti i reati attualmente ricompresi nell'ambito di applicazione del Decreto.

III. Criteri di imputazione della responsabilità dell'Ente

Nel caso di commissione di uno dei Reati, l'Ente può essere considerato responsabile in presenza di determinate condizioni, qualificabili quali "criteri di imputazione dell'Ente". I criteri per l'attribuzione della responsabilità all'Ente sono "oggettivi" e "soggettivi".

I criteri di natura *oggettiva* prevedono che gli Enti possono essere considerati responsabili ogniqualvolta si

realizzino i comportamenti illeciti tassativamente elencati nel Decreto purché:

a) il reato sia stato commesso ***nell'interesse*** o ***a vantaggio*** dell'Ente;

b) il reato sia stato commesso:

i. "*da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo degli stessi*" (cosiddetti "**Soggetti Apicali"**);

ii. "*da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)*" (cosiddetti "**Soggetti Subordinati"**).

Per quanto attiene alla nozione di "interesse", esso si concretizza ogniqualvolta la condotta illecita sia posta in essere con l'intento di procurare un beneficio alla Società; la medesima responsabilità è del pari ascrivibile alla Società ogniqualvolta la stessa tragga dalla condotta illecita un qualche *vantaggio* (economico/patrimoniale o non) di tipo indiretto, pur avendo l'autore del reato agito senza il fine esclusivo di recare un beneficio alla persona giuridica. Al contrario, la responsabilità dell'Ente è esclusa nel caso in cui il Reato, seppur compiuto con violazione delle disposizioni del Modello, non abbia comportato alcun vantaggio né sia stato commesso nell'interesse dell'Ente, bensì a interesse e vantaggio esclusivo dell'autore della condotta criminosa.

L'interesse e il vantaggio dell'Ente sono due criteri alternativi e perché sussista la responsabilità dell'Ente è sufficiente che ricorra almeno uno dei due. La legge non richiede che il beneficio ottenuto o sperato dall'Ente sia necessariamente di natura economica: la responsabilità sussiste non soltanto allorché il comportamento illecito abbia determinato un vantaggio patrimoniale, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il reato intenda favorire l'interesse dell'Ente. L'Ente non risponde invece se il reato è stato commesso indipendentemente o contro il suo interesse oppure nell'interesse esclusivo dell'autore del reato o di terzi. Gli articoli 6 e 7 del Decreto disciplinano i criteri di imputazione soggettiva della responsabilità dell'Ente, i quali variano a seconda che a realizzare il Reato sia un Soggetto Apicale o un Soggetto Subordinato.

L'interesse può essere rilevato anche nell'ambito di un gruppo di imprese, nel senso che la controllante potrà essere ritenuta responsabile per il Reato commesso nell'attività della controllata qualora sia ravvisabile anche un interesse o vantaggio della controllante.

Tuttavia, perché possa ricorrere la responsabilità della controllante è necessario che:

- l'interesse o vantaggio della controllante sia immediato e diretto, ancorché non patrimoniale;
- il soggetto che ha concorso a commettere il Reato (con un contributo causalmente rilevante provato in concreto) sia funzionalmente collegato alla Società.

Con riferimento ai Reati colposi, quali l'omicidio o le lesioni personali gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (ex art. 25-*septies* del Decreto) e taluni reati ambientali (ex art. 25-*undecies* del Decreto), l'interesse e/o il vantaggio dell'Ente non andranno riferiti all'evento (quale, a titolo di esempio, la morte del lavoratore), ma alla condotta causativa di tale evento, purché consapevoli e volontarie finalizzate a favorire l'Ente[2].

Pertanto, l'interesse e/o il vantaggio potranno ravvisarsi nel risparmio di costi per la sicurezza ovvero nel potenziamento della velocità di esecuzione delle prestazioni o nell'incremento della produttività conseguenti alla mancata adozione delle necessarie tutele infortunistiche o ambientali imposte dall'ordinamento.

[2] Non rileverebbero, quindi, ai fini della responsabilità dell'ente le condotte derivanti da semplice imperizia, mera sottovalutazione del rischio o imperfetta esecuzione delle misure antinfortunistiche.

L'Ente non risponde invece se il Reato è stato commesso indipendentemente o contro il suo interesse oppure nell'interesse esclusivo dell'autore del reato o di terzi.

Gli articoli 6 e 7 del Decreto disciplinano i criteri di imputazione soggettiva della responsabilità dell'Ente, che variano a seconda che a realizzare il Reato sia un Soggetto Apicale o un Soggetto Subordinato.

Nel caso di Reati commessi da Soggetti Apicali, l'articolo 6 del Decreto prevede una forma specifica di esonero dalla responsabilità dell'Ente, qualora lo stesso dimostri che:

- il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curare il suo aggiornamento, è stato affidato all'Organismo di Vigilanza;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza;
- le persone che hanno commesso il reato hanno agito eludendo fraudolentemente le misure previste dal Modello[3].

Le condizioni sopra elencate devono concorrere congiuntamente affinché la responsabilità dell'Ente possa essere esclusa; l'esenzione dell'Ente da responsabilità dipende quindi dalla prova da parte dell'Ente medesimo dell'adozione ed efficace attuazione di un Modello di prevenzione dei Reati e della istituzione di un OdV.

Nel caso invece di Reati commessi da un Soggetto Subordinato, l'articolo 7 del Decreto prevede che l'Ente sarà chiamato a rispondere solo nell'ipotesi in cui il Reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza, inosservanza che si considera esclusa se l'Ente, prima della commissione del Reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire i Reati.

Con specifico riferimento alla materia della salute e sicurezza sul luogo di lavoro, l'art. 30 del D.Lgs. 9 aprile 2008, n. 81, stabilisce che il Modello idoneo ad avere efficacia esimente della responsabilità amministrativa degli enti di cui al Decreto deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

Il Modello deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività in precedenza elencate. Il Modello deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche

[3] La frode cui fa riferimento il Decreto non necessariamente richiede artifici o raggiri ma presuppone che la violazione del Modello sia determinata da un aggiramento dei presidi di controllo in esso previsti che sia idoneo a "forzarne" l'efficacia.

e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello. Il Modello deve altresì prevedere un idoneo sistema di controllo sull'attuazione dello stesso e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

Infine, il suddetto art. 30 stabilisce che, in sede di prima applicazione, i Modelli elaborati conformemente a:

- le Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001; ovvero
- il *British Standard* OHSAS 18001:2007 e il nuovo standard ISO 45001:2018;

si presumono conformi ai requisiti più sopra enunciati per le parti corrispondenti.

La presunzione di conformità si riferisce alla valutazione di astratta idoneità preventiva del modello legale, ma non anche alla efficace attuazione, che verrà effettuata dal giudice sulla base dell'osservanza concreta e reale dell'effettiva implementazione del Modello[4].

IV. Le sanzioni previste dal Decreto

Il sistema sanzionatorio, a fronte del compimento dei reati sopra elencati, prevede l'applicazione delle seguenti sanzioni amministrative:

a) sanzioni pecuniarie;
b) sanzioni interdittive;
c) confisca;
d) pubblicazione della sentenza.

a) Sanzioni pecuniarie

In caso di condanna dell'ente, è sempre applicata la sanzione pecuniaria. La sanzione pecuniaria è determinata dal giudice attraverso un sistema basato su quote. Il numero delle quote (che vanno da un numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 ad un massimo di Euro 1.549,00) dipende dalla gravità del reato, dal grado di responsabilità dell'ente, dall'attività svolta per eliminare e attenuare le conseguenze del fatto o per prevenire la commissione degli atti illeciti. Al fine di rendere efficace la sanzione, l'importo della quota, inoltre, è determinato dal Giudice sulla base delle condizioni economiche e patrimoniali dell'Ente.

La sanzione pecuniaria è ridotta nel caso in cui: a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità, o se, prima della dichiarazione di apertura del dibattimento in primo grado: c) l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso e d) un Modello è stato adottato e reso operativo.

b) Sanzioni interdittive

Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni: a) l'Ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti che ricoprono una posizione di rappresentanza, amministrativa o di gestione nell'Ente ovvero da soggetti sottoposti alla direzione e al controllo dei primi e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; o b) in caso di reiterazione degli illeciti.

Il Decreto prevede le seguenti sanzioni interdittive, che possono avere una durata non inferiore a tre mesi e

[4] La conformità dell'Ente ai sistemi di certificazione non costituisce presunzione di conformità ai requisiti del Decreto.

non superiore a due anni:

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

Ai sensi della vigente normativa, le sanzioni interdittive non si applicano in caso di commissione dei reati societari e di market abuse. Si precisa infatti che, per tali reati, sono previste le sole sanzioni pecuniarie, raddoppiate nel loro ammontare dall'art. 39, comma 5, della L. 262/2005 ("Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari").

Il Decreto prevede, inoltre, che, qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione interdittiva, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Una volta accertata la sussistenza di uno dei due presupposti, il giudice con sentenza dispone la prosecuzione dell'attività dell'ente da parte di un commissario, indicandone i compiti e i poteri con particolare riferimento alla specifica area in cui è stato commesso l'illecito; il commissario cura quindi l'azione di modelli organizzativi idonei a prevenire la commissione di reati della specie di quello verificatosi e non può compiere atti di straordinaria amministrazione senza autorizzazione del giudice.

Nonostante la tutela della collettività, il commissario giudiziale è pur sempre un'alternativa alla sanzione interdittiva ed è per questo che deve possedere un carattere sanzionatorio; ciò avviene mediante la confisca del profitto derivante dalla prosecuzione dell'attività. Infine è bene precisare come la soluzione del commissario giudiziale non possa essere adottata in caso di applicazione di una sanzione interdittiva in via definitiva.

Le sanzioni interdittive sono normalmente temporanee, ma nei casi più gravi possono eccezionalmente essere applicate con effetti definitivi.

L'art. 16 del D. Lgs. 231/2001 definisce quando la sanzione interdittiva va applicata in via definitiva: l'interdizione definitiva dall'esercizio dell'attività può essere applicata se l'ente ha tratto dal reato un profitto di un certo rilievo ed è già stato condannato, almeno tre volte negli ultimi sette anni, all'interdizione temporanea dall'esercizio dell'attività. Il giudice, inoltre, può applicare all'ente in via definitiva la sanzione del divieto di contrattare con la pubblica amministrazione o del divieto di pubblicizzare beni o servizi, quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni. Infine in caso di impresa illecita, ossia un'organizzazione con l'unico scopo di consentire o agevolare la commissione di reati, deve essere sempre applicata l'interdizione definitiva dall'esercizio dell'attività.

Inoltre le sanzioni interdittive possono essere applicate anche in via cautelare, ovvero prima della condanna, qualora sussistano gravi indizi della responsabilità dell'ente e vi siano fondati e specifici elementi tali da far ritenere il concreto pericolo che vengano commessi illeciti della stessa tipologia di quello per cui si procede. Le sanzioni interdittive non si applicano se la sanzione pecuniaria è in formula ridotta.

Le sanzioni interdittive, tuttavia, non si applicano qualora l'ente, prima della dichiarazione di apertura del dibattimento di primo grado:

- abbia risarcito il danno ed eliminato le conseguenze dannose o pericolose del reato (o almeno si sia efficacemente adoperato in tal senso);
- abbia messo a disposizione dell'autorità giudiziaria il profitto del reato;

- abbia eliminato le carenze organizzative che hanno determinato il reato adottando e attuando effettivamente ed in modo efficace adeguati modelli organizzativi idonei a prevenire la commissione di nuovi reati della specie di quello verificatosi.

Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinati dal Giudice penale competente, tenendo conto di quanto previsto dall'art. 14 del Decreto.

Le sanzioni interdittive hanno una durata che varia da un minimo di tre mesi a un massimo di sette anni.

Le sanzioni interdittive devono essere riferite allo specifico settore di attività dell'ente e devono rispondere ai principi di adeguatezza, proporzionalità e sussidiarietà, in particolare ove applicate in via cautelare.

c) Confisca

La confisca del prezzo o del profitto del Reato è sempre disposta dal Giudice penale con la sentenza di condanna, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede[5].

Quando non è possibile eseguire la confisca del prezzo o del profitto del Reato, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del Reato.

d) Pubblicazione della sentenza

Il giudice penale può disporre la pubblicazione della sentenza di condanna quando nei confronti dell'Ente viene applicata una sanzione interdittiva.

La sentenza è pubblicata ai sensi dell'art. 36 c.p., nonché mediante affissione nel Comune ove l'Ente ha la sede principale.

V. Condizione esimente della Responsabilità amministrativa

Il Decreto prevede espressamente, agli artt. 6 e 7, l'esenzione dalla responsabilità amministrativa dell'Ente per reati commessi a proprio vantaggio e/o interesse qualora l'ente si sia dotato di effettivi ed efficaci modelli di organizzazione, gestione e controllo (di seguito anche il "Modello"), idonei a prevenire i medesimi fatti illeciti richiamati dalla normativa.

In particolare, nel caso in cui il reato venga commesso da Soggetti Apicali, l'Ente non risponde se prova che:

- l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curare il loro aggiornamento è stato affidato a un Organismo di Vigilanza dell'Ente dotato di autonomi poteri di iniziativa e controllo;
- le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione e gestione;
- vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza incaricato di vigilare sul funzionamento e sull'osservanza dei modelli di organizzazione e di gestione.

Per i reati commessi dai Sottoposti, l'Ente può essere chiamato a rispondere solo qualora venga accertato che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. In questa ipotesi, il Decreto riconduce la responsabilità ad un inadempimento dei doveri di direzione e vigilanza, che gravano tipicamente sul vertice aziendale (o sui soggetti da questi delegati).

L'inosservanza degli obblighi di direzione o vigilanza non ricorre se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

La semplice adozione del Modello da parte dell'organo dirigente non è, tuttavia, misura sufficiente a determinare l'esonero da responsabilità dell'ente medesimo, essendo piuttosto necessario che il Modello sia

[5] Ai fini della confisca si deve far riferimento al momento di realizzazione del reato e non a quello di percezione del profitto, così che non sarà suscettibile di confisca il profitto derivante da un reato che non era al momento di realizzazione della condotta incluso nel novero dei reati presupposto di cui al Decreto (ma lo era al momento di conseguimento del profitto).

anche idoneo, efficace ed effettivo. A tal proposito il Decreto indica le caratteristiche essenziali per la costruzione di un modello di organizzazione gestione e controllo.

In particolare, per la prevenzione dei reati il Modello deve (art. 6 comma 2 del Decreto):

- individuare e definire le attività aziendali nel cui ambito esiste la possibilità che vengano commessi reati previsti dal Decreto;
- predisporre specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- stabilire le modalità di reperimento e di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato a vigilare sul funzionamento e sull'osservanza del modello di organizzazione, gestione e controllo, al fine di consentirne la concreta capacità operativa;
- predisporre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo, al fine di garantirne l'effettività.

Inoltre, con riferimento all'efficace attuazione del Modello si prevede (art. 7 comma 4):

- una verifica periodica e l'eventuale modifica del Modello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
- l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

A tali requisiti devono aggiungersi, con riferimento ai reati commessi con violazione della normativa in materia di salute e sicurezza sul lavoro, quelli specificatamente dettati dall'art. 30, comma 1, del D.lgs. 9 aprile 2008, 81 ("**D.lgs. 81/08**"), secondo cui il Modello organizzativo deve essere tale da assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

Il Modello deve, inoltre, prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra descritte, nonché un'articolazione di funzioni tale da assicurare le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve, altresì, prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni

significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

VI. Le "Linee Guida" di Confindustria

L'art. 6 del Decreto dispone espressamente che il Modello possa essere adottato sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Le Linee Guida di Confindustria sono state approvate dal Ministero della Giustizia con il D.M. 4 dicembre 2003. Il successivo aggiornamento, pubblicato da Confindustria in data 24 maggio 2004, è stato approvato dal Ministero della Giustizia, che ha giudicato tali Linee Guida idonee al raggiungimento delle finalità previste dal Decreto. Dette Linee Guida sono state aggiornate da Confindustria alla data di marzo 2014.

Nella definizione del Modello, le Linee Guida di Confindustria prevedono le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare i reati previsti dal Decreto;
- la predisposizione di un sistema di controllo[6] (i c.d. protocolli) idoneo a prevenire i rischi di reato identificati nella fase precedente, attraverso la valutazione del sistema di controllo esistente all'interno dell'ente ed il suo grado di adeguamento alle esigenze espresse dal Decreto.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida di Confindustria per garantire l'efficacia del modello di organizzazione, gestione e controllo, sono le seguenti:

- la previsione di principi etici e di regole comportamentali in un codice etico;
- un sistema organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e descrizione dei compiti con specifica previsione di principi di controllo;
- procedure, manuali e/o informatiche, che regolino lo svolgimento delle attività, prevedendo opportuni controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, laddove richiesto, l'indicazione di limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

Il sistema di controllo, inoltre, deve conformarsi ai seguenti principi:

- verificabilità, tracciabilità, coerenza e congruità di ogni operazione;
- segregazione dei compiti (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli effettuati.

VII. Delitti tentati e delitti commessi all'estero

L'Ente risponde anche degli illeciti dipendenti da delitti tentati e da reati commessi all'estero.

Nelle ipotesi di commissione nella forma del tentativo dei delitti previsti dal 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. L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto.

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere, in relazione a reati – contemplati dallo stesso Decreto – commessi all'estero, al fine di non lasciare sfornita di

---

[6] Il sistema di controllo esistente all'interno dell'ente, o sistema di controllo interno, "*è l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati*" (v. Codice di Autodisciplina, Comitato per la *Corporate Governance*, Borsa Italiana S.p.A., 2006, pag. 35).

sanzione una condotta criminosa di frequente verificazione, 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:

- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;
- l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
- le condizioni previste dagli artt. 7, 8, 9, 10 codice penale, con riferimento alla punibilità dei reati commessi all'estero, si devono essere verificate (nell'Allegato B – "Articoli del Codice Penale richiamati dall'art. 4 del D.Lgs. 231/2001", sono descritte le fattispecie dei reati);
- non si procede nei confronti dell'Ente nello Stato in cui è stato commesso il fatto.

4 Il Modello di Organizzazione, Gestione e Controllo di TeamSystem S.p.A.

I. La Società

Con una presenza capillare e diffusa su tutto il territorio nazionale, TeamSystem S.p.A. (di seguito anche TeamSystem o la "Società") offre software e servizi ai clienti, sia direttamente attraverso le proprie sedi sia indirettamente attraverso una rete di Software Partner selezionati.

La Società, fondata nel 1979, è cresciuta costantemente negli anni a seguire sino a diventare un operatore di riferimento nel mercato delle soluzioni digitali per la gestione del business di imprese, professionisti (commercialisti, consulenti del lavoro, avvocati) e delle associazioni.

TeamSystem S.p.A. è una società registrata presso l'Ufficio del Registro di Pesaro, ove ha sede oltre che in ulteriori sedi dislocate nelle principali città italiane. TeamSystem S.p.A. è leader in Italia nella produzione e nella commercializzazione di software gestionali/ERP e nei servizi di formazione rivolti alle micro, piccole e medie imprese; ai professionisti (commercialisti, consulenti del lavoro, avvocati, amministratori di condominio e liberi professionisti) ed alle associazioni.

La rete commerciale e tecnica è costituita da professionisti altamente specializzati e con specifiche competenze di settore, in grado non solo di fornire un'assistenza al cliente di elevata qualità, ma anche di garantire la massima efficacia e personalizzazione delle soluzioni sulla base delle specifiche esigenze dell'utente finale.

La Società è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri soci e del lavoro dei propri dipendenti ed è consapevole dell'importanza di dotarsi di un sistema di controllo interno aggiornato ed idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, rappresentanti e partner d'affari.

Al fine di realizzare tale obiettivo, la Società ha da tempo adottato un sistema di governance aziendale articolato e rispondente alla miglior prassi internazionale.

In ragione di quanto precede, la Società ha ritenuto conforme alle proprie politiche aziendali ed ai propri obiettivi verificare ed adeguare i principi comportamentali e le procedure già adottate alle finalità previste dal Decreto e ad implementare il Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/01 (di seguito il "Modello").

Attraverso l'adozione del Modello, TeamSystem intende perseguire i seguenti obiettivi:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- diffondere la consapevolezza che dalla violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie (di natura pecuniaria e interdittiva) anche a carico della Società;
- consentire alla Società, grazie ad un sistema strutturato di procedure e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

II. Modello di Governance

La corporate governance di TeamSystem, basata sul modello tradizionale, è così articolata:

Assemblea degli azionisti, competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o 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 degli atti riservati – dalla legge e dallo statuto – all'Assemblea.

Collegio Sindacale, cui spetta il compito di vigilare: a) sull'osservanza della legge e dallo statuto nonché sul rispetto dei principi di corretta amministrazione; b) 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; c) 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 speciale della Consob, che svolge l'attività di revisione contabile, incaricata dall'Assemblea degli azionisti.

III. Finalità del Modello

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventivo ed ex post) che abbia come obiettivo la riduzione del rischio di commissione dei reati mediante l'individuazione delle "Aree di a rischio" e delle "Attività sensibili" alla commissione dei reati e la loro conseguente proceduralizzazione.

I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza nel potenziale autore del reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi di TeamSystem anche quando apparentemente essa potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a TeamSystem di reagire tempestivamente nel prevenire od impedire la commissione del reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare la consapevolezza nei Dipendenti, Organi Sociali, Società di Service, Consulenti e Partner, che operino per conto o nell'interesse della Società nell'ambito delle "Aree di rischio" e delle "Attività sensibili", di poter incorrere - in caso di comportamenti non conformi alle prescrizioni del Codice Etico e alle altre norme e procedure aziendali – in illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società.

Inoltre, si intende censurare fattivamente ogni comportamento illecito attraverso la costante attività dell'Organismo di Vigilanza sull'operato delle persone rispetto alle "Aree di rischio" e alle "Attività sensibili" e la comminazione di sanzioni disciplinari o contrattuali.

Gli elementi che caratterizzano il presente Modello sono: l'**efficacia**, la **specificità** e l'**attualità**.

a) Efficacia

L'efficacia di un Modello dipende dalla sua idoneità in concreto ad elaborare meccanismi di decisione e di controllo tali da eliminare, o quantomeno ridurre significativamente, l'area di rischio da responsabilità. Tale idoneità è garantita dall'esistenza di meccanismi di controllo preventivo e successivo idonei ad identificare le operazioni che possiedono caratteristiche anomale, tali da segnalare condotte rientranti nelle aree di rischio e strumenti di tempestivo intervento nel caso di individuazione di siffatte anomalie. L'efficacia di un Modello, infatti, è anche funzione dell'efficienza degli strumenti idonei ad identificare "sintomatologie da illecito".

b) Specificità

La specificità di un Modello è uno degli elementi che ne connota l'efficacia.

- È necessaria una specificità connessa alle aree a rischio, così come richiamata dall'art. 6, comma 2 lett.a) del Decreto, che impone un censimento delle attività della Società nel cui ambito possono essere commessi i reati;
- Ai sensi dell'art. 6, comma 2 lett.b) del Decreto, è altrettanto necessario che il Modello preveda dei processi specifici di formazione delle decisioni dell'ente e dei processi di attuazione nell'ambito dei settori "sensibili".

Analogamente, l'individuazione delle modalità di gestione delle risorse finanziarie, l'elaborazione di un sistema di doveri d'informativa, l'introduzione di un adeguato sistema disciplinare sono obblighi che richiedono la specificità delle singole componenti del Modello.

Il Modello, ancora, deve tener conto delle caratteristiche proprie, delle dimensioni della Società e del tipo di attività svolte, nonché della storia della Società.

c) Attualità

Un Modello è idoneo a ridurre i rischi da reato qualora sia costantemente adattato ai caratteri della struttura e dell'attività d'impresa.

In tal senso l'art. 6 del Decreto prevede che l'Organismo di Vigilanza, titolare di autonomi poteri d'iniziativa e controllo, abbia la funzione di supervisionare all'aggiornamento del Modello.

L'art. 7 del Decreto stabilisce che l'efficace attuazione del Modello contempli una verifica periodica, nonché l'eventuale modifica dello stesso allorquando siano scoperte eventuali violazioni oppure intervengano modifiche nell'attività o nella struttura organizzativa della Società.

IV. Destinatari

Le regole contenute nel Modello si applicano:

- a coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale, amministratore, membro del collegio sindacale;
- a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società o in una sua unità organizzativa autonoma;
- a coloro i quali svolgano funzioni di direzione in veste di responsabili di specifiche Unità Organizzative;
- a coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società;
- ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale, ancorché distaccati all'estero per lo svolgimento dell'attività;
- ai Dipendenti della Società, anche se distaccati all'estero per lo svolgimento delle attività;
- a tutti quei soggetti che collaborano con la Società in forza di un rapporto di lavoro parasubordinato, quali collaboratori a progetto, prestatori di lavoro temporaneo, interinali, etc.;
- a chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima.
- a quei soggetti che agiscono nell'interesse della Società, in quanto legati alla stessa da rapporti giuridici contrattuali o da accordi di altra natura, quali, ad esempio, *partner* in *joint-venture* o soci per la realizzazione o l'acquisizione di un progetto di *business*.
- a tutti i soggetti del Gruppo le cui attività/decisioni abbiano un impatto sulla Società.

Il Modello costituisce un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di materiali, servizi e lavori, consulenti, *partners* con cui TeamSystem opera.

V. Struttura del Modello

Il Modello è formato da tutte le "componenti" individuate nel paragrafo VI che segue e da tutte le procedure, le *policies* aziendali e di gruppo ed i sistemi di gestione e controllo richiamati e/o previsti nel presente documento.

Il presente documento è composto da una Parte Generale e dalla Parte Speciale.

La **Parte Generale** ha ad oggetto la descrizione della disciplina contenuta nel D.Lgs. 231/01, l'indicazione – nelle parti rilevanti ai fini del Decreto – della normativa specificamente applicabile alla Società, la descrizione dei reati rilevanti per la Società, l'indicazione dei destinatari del Modello, i principi di funzionamento dell'Organismo di Vigilanza, la definizione di un sistema sanzionatorio dedicato al presidio delle violazioni del Modello, l'indicazione degli obblighi di comunicazione del Modello e di formazione del personale.

La **Parte Speciale** ha ad oggetto l'indicazione delle aree di rischio e delle relative attività "sensibili", cioè delle attività che sono state considerate dalla Società a rischio di reato, in esito alle analisi dei rischi condotte, ai sensi del Decreto, i principi generali di comportamento, gli elementi di prevenzione a presidio delle suddette attività e le misure di controllo essenziali deputate alla prevenzione o alla mitigazione degli illeciti.

Costituiscono inoltre parte integrante del Modello:

- il *Risk Self Assessment* finalizzato all'individuazione delle attività sensibili;
- il Codice Etico, che definisce i principi e le norme di comportamento della Società;
- il Codice di Condotta Anticorruzione, che contiene i principi e le regole di comportamento che la Società si è data nello specifico ambito della lotta alla corruzione;

- tutte le disposizioni, i provvedimenti interni, gli atti o le procedure operative aziendali che costituiscono gli strumenti di attuazione del Modello.

Tali atti e documenti sono reperibili, secondo le modalità previste per la loro diffusione, all'interno dell'azienda e sulla intranet aziendale.

E' opportuno precisare che il presente documento individua e riassume il contenuto descrittivo ed i principi generali di adozione del Modello, essendo l'individuazione dei sistemi di prevenzione dei rischi concretamente definita anche attraverso il rinvio agli strumenti di controllo utilizzati nella realtà operativa aziendale (tra cui procedure, istruzioni operative, policies, sistemi autorizzativi, struttura organizzativa, sistema delle deleghe e delle procure, norme di comportamento, modalità di gestione delle risorse finanziarie, strumenti di tracciabilità e documentazione, etc.), da intendersi integralmente richiamati nel presente Modello. Ed infatti, ragioni di "praticabilità" e funzionalità dello stesso Modello Organizzativo impongono di non trascrivere pedissequamente e materialmente all'interno del presente documento l'intero sistema delle procedure e degli ulteriori controlli in essere, tanto più ove si consideri che tali strumenti di controllo operativo costituiscono un "corpo vivo", dinamico ed in costante evoluzione, soggetto ad esigenze di aggiornamento proprio allo scopo di garantirne l'efficacia e l'attualità. Ciononostante, tali procedure e sistemi di controllo devono intendersi qui richiamati quale parte integrante ed essenziale del Modello Organizzativo, del quale costituiscono il nucleo "operativo".
Anche le azioni di miglioramento del sistema di controllo interno attuate successivamente all'adozione del Modello Organizzativo costituiscono a tutti gli effetti parte integrante del Modello Organizzativo stesso, nonché del sistema dei protocolli preventivi adottati a presidio delle diverse aree ed attività a rischio.

VI. Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali sviluppati da TeamSystem nella definizione del Modello, possono essere così riassunti:

- mappatura delle attività sensibili[7], con esempi di possibili modalità di realizzazione dei reati e dei processi strumentali/funzionali potenzialmente associabili alla commissione dei reati richiamati dal Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico;
- identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal Decreto, sancite nel Codice Etico adottato dalla Società e, più in dettaglio, nel presente Modello;
- nomina di un Organismo di Vigilanza al quale sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello ai sensi dell'art. 6 punto b) del Decreto;
- approvazione di un sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione, sensibilizzazione e divulgazione ai Destinatari del presente Modello;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso.

VII. Codice Etico e Modello

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice stesso. Sotto tale profilo, infatti:

[7] Tramite l'analisi documentale e le interviste svolte, con i soggetti aziendali informati dell'organizzazione e delle attività svolte dalle Funzioni/Direzioni, nonché dei processi aziendali nei quali le attività sono articolate, sono identificate le aree di rischio alla commissione dei reati, o aree di attività a potenziale rischio-reato ai sensi del Decreto e le relative attività sensibili.

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte della Società allo scopo di esprimere dei principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti;
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi apparentemente a vantaggio dell'azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

VIII. Presupposti del Modello

Nella predisposizione del Modello, TeamSystem ha tenuto conto della propria organizzazione aziendale, al fine di verificare le aree di attività più esposte al rischio di potenziale commissione di reati.

La Società ha tenuto altresì conto del proprio sistema di controllo interno al fine di verificarne la capacità a prevenire le fattispecie di reato previste dal Decreto nelle aree di attività identificate a rischio.

Più in generale, il sistema di controllo interno di TeamSystem deve garantire, con ragionevole certezza, il raggiungimento di obiettivi operativi, di informazione e di conformità:

- l'obiettivo operativo del sistema di controllo interno riguarda l'efficacia e l'efficienza della Società nell'impiegare le risorse, nel proteggersi dalle perdite, nel salvaguardare il patrimonio aziendale; tale sistema è volto, inoltre, ad assicurare che il personale operi per il perseguimento degli obiettivi aziendali, senza anteporre altri interessi a quelli di TeamSystem;
- l'obiettivo di informazione si traduce nella predisposizione di rapporti tempestivi ed affidabili per il processo decisionale all'interno e all'esterno dell'organizzazione aziendale;
- l'obiettivo di conformità garantisce, invece, che tutte le operazioni ed azioni siano condotte nel rispetto delle leggi e dei regolamenti, dei requisiti prudenziali e delle procedure aziendali interne.

Con l'adozione del Modello, la Società ha inteso completare e perfezionare il proprio sistema di *governance* aziendale - rappresentato da un complesso strutturato e organico di regole, codici di comportamento, procedure e sistemi di controllo – al fine di poter prevenire la commissione delle diverse tipologie di reati contemplate dal Decreto e considerate rilevanti dalla Società.

L'adozione del Modello organizzativo, in particolare, ha comportato l'integrazione del sistema di *policy,* procedure e controlli in essere - laddove ritenuto opportuno - al fine di adeguarlo al rispetto dei seguenti principi fondamentali:

i. verificabilità, documentabilità, coerenza e congruità di ogni operazione;
ii. separazione delle funzioni coinvolte nella gestione di ciascun processo;
iii. chiara definizione e formalizzazione delle responsabilità e dei poteri attribuiti dalla Società;
iv. necessità che ciascuna operazione significativa trovi origine in un'adeguata autorizzazione interna;
v. previsione di limiti all'esercizio di poteri in nome e per conto della Società;
vi. coerenza tra i poteri formalmente conferiti e quelli concretamente esercitati nell'ambito dell'organizzazione della Società;
vii. coerenza tra i sistemi di controllo (ivi comprese le procedure, la struttura organizzativa, i processi ed i sistemi informativi), il Codice Etico e le regole di comportamento adottate dalla Società;
viii. documentazione e documentabilità dei controlli effettuati.

Coerentemente ai principi sopra espressi, il sistema di *governance* di TeamSystem si compone degli elementi di seguito sinteticamente considerati:

IX. Codice Etico

Il Codice Etico della Società fissa i principi di condotta e le linee generali di comportamento che i responsabili di funzione, i dirigenti, i dipendenti e tutti coloro che collaborano con la Società sono tenuti a rispettare nello svolgimento delle proprie attività.

Il Codice Etico, che costituisce il fondamento del sistema di controllo interno di TeamSystem, è concepito come "carta dei valori" contenente i principi generali che uniformano l'attività di impresa e che si traducono in altrettante regole di comportamento orientate all'etica. L'insieme di tali regole, avente carattere volutamente generale e di immediata percepibilità, persegue lo scopo dichiarato di evitare comportamenti scorretti o ambigui attraverso una chiara enunciazione delle regole da rispettare, con l'avvertenza che in caso di violazione i destinatari potranno essere sanzionati.

X. Struttura organizzativa

La struttura organizzativa della Società è articolata secondo una ripartizione definita delle competenze e dei ruoli, assegnati in conformità al sistema di deleghe/procure in essere.

Negli organigrammi societari vengono individuate le aree (Direzioni) in cui si scompone l'attività aziendale, le linee di dipendenza gerarchica, i soggetti assegnati alle singole aree e i ruoli organizzativi che ad essi competono.

La distribuzione dei ruoli e delle funzioni è improntata al principio della separazione dei poteri e alla coerenza tra le responsabilità formalmente assegnate e quelle in concreto assunte da ciascun soggetto nell'ambito della compagine organizzativa.

In caso di mutamenti organizzativi, la Società provvede a modificare ed integrare gli organigrammi aziendali e la ripartizione delle competenze e funzioni tra le proprie divisioni.

Con specifico riguardo ai reati in materia di salute e sicurezza dei lavoratori, la Società si è dotata di una struttura organizzativa interna ed ha provveduto a definire i ruoli e le responsabilità in materia di sicurezza secondo quanto previsto dalla vigente normativa, in particolare dal D.lgs. 81/2008.

Tale struttura organizzativa risulta schematizzata nell'organigramma aziendale per la sicurezza, allegato al Documento di Valutazione dei rischi (DVR), tempestivamente aggiornato in caso di mutamenti organizzativi e divulgato a tutti i livelli tramite gli strumenti informativi aziendali.

XI. Sistema autorizzativo

La Società ha adottato un sistema formalizzato di deleghe gestionali interne per l'esercizio di rappresentanza e di spesa, da esercitarsi coerentemente con le competenze gestionali e le responsabilità organizzative affidate all'interno dell'organizzazione aziendale.

Le deleghe ad agire e le procure a spendere sono conferite dal Consiglio di Amministrazione.

L'attribuzione di poteri di rappresentanza della Società è, in ogni caso, effettuata in modo da garantire la coerenza tra i poteri conferiti ed le responsabilità organizzative e gestionali effettivamente assegnate all'interno dell'organizzazione. Al fine di assicurare il costante aggiornamento del sistema autorizzativo, è previsto l'aggiornamento del sistema di deleghe e procure qualora ciò si renda necessario a seguito di mutamenti organizzativi (es. variazioni di responsabilità o attribuzione di nuove competenze), così come in caso di uscita dall'organizzazione aziendale di procuratori e/o delegati o di ingresso di nuovi soggetti che necessitano di poteri formali per l'esercizio delle proprie responsabilità.

XII. Sistema di controllo di gestione e reporting

Le modalità di gestione delle risorse finanziarie individuate dalla Società assicurano la separazione 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.

Sono stabiliti limiti all'autonomia decisionale per l'impiego delle risorse finanziarie mediante soglie quantitative

in coerenza con le competenze gestionali e le responsabilità organizzative affidate all'interno della Società.

Il sistema di controllo di gestione prevede procedure atte alla verifica dell'impiego delle risorse; tali procedure sono, peraltro, volte a garantire una completa tracciabilità delle spese anche ai fini del mantenimento di un'adeguata efficienza ed economicità delle attività aziendali.

La gestione finanziaria è oggetto di pianificazione tramite il budget societario, inserito nel sistema di reporting agli azionisti ed assoggettato a monitoraggio mensile sotto la responsabilità del Controllo di Gestione.

XIII. Sistema di gestione della qualità e della sicurezza delle informazioni

La Società si è dotata di un sistema organizzativo e gestionale che soddisfa i seguenti standard internazionali:

i) la norma UNI EN ISO 9001:2008 in materia di qualità del prodotto;
ii) ISO/IEC 27001:2013 e ISO/IEC 27018 in materia di gestione della sicurezza delle informazioni con riferimento all'erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura cloud Iaas;

Tali sistemi certificati contribuiscono a dare chiara evidenza ai processi aziendali interessati e a garantirne il costante miglioramento nel tempo, oltre a portare, anche attraverso gli *audit* e i controlli eseguiti con frequenza programmata, una maggiore attenzione sul rispetto delle procedure e istruzioni relative.

In proposito, se pure l'adozione di tali sistemi di gestione non consente di esaurire i requisiti di idoneità dei modelli organizzativi ai sensi del D.lgs. 231/2001, si ritiene comunque che gli stessi costituiscano un importante presidio che si integra nel più ampio quadro dei controlli previsti dallo stesso Modello Organizzativo.

XIV. Procedure manuali ed informatiche

L'attività della Società è regolata da una serie di *policies* e procedure, manuali ed informatiche, che indicano le modalità operative dell'attività lavorativa e i relativi sistemi di controllo. Dette procedure regolano, nello specifico, le modalità di svolgimento dei processi aziendali, prevedendo anche i controlli da espletare al fine di garantire la correttezza, la trasparenza e la verificabilità delle attività aziendali.

Le procedure interne sono caratterizzate dai seguenti elementi:

- separazione, per quanto possibile, all'interno di ciascun processo, tra il soggetto che assume la decisione, il soggetto che la autorizza, il soggetto che esegue tale decisione ed il soggetto cui è affidato il controllo del processo;
- tracciabilità di ciascun passaggio rilevante del processo, incluso il controllo;
- adeguato livello di formalizzazione.

Il sistema di procedure è supportato da un sistema di gestione amministrativo-contabile in grado di garantire una tempestiva rappresentazione di tutti i flussi economici e finanziari riconducibili all'attività caratteristica della Società e ad eventuali attività non caratteristiche.

Tali procedure sono rese disponibili a tutti i dipendenti attraverso la rete *intranet* aziendale, oltre che attraverso specifiche attività di *training* eseguite nell'ambito di ciascuna unità organizzativa in caso di emendamento o aggiornamento delle procedure.

XV. Modifiche del Modello

Tutte le modifiche e le integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del Consiglio di Amministrazione della Società, essendo il presente Modello un atto di emanazione dell'organo dirigente (cfr. Decreto, Art. 6).

Al fine di garantire la stabilità e l'effettività del Modello, le decisioni per le modifiche ed integrazioni sostanziali del Modello devono essere approvate con il voto favorevole di almeno due terzi degli amministratori presenti alla seduta.

XVI. Le attività propedeutiche all'adozione del Modello Organizzativo

La predisposizione del Modello è stata preceduta da una serie di attività propedeutiche in linea con le previsioni del Decreto.

Il Decreto prevede espressamente, al relativo art. 6, comma 2, lett. a), che il Modello dell'ente individui, infatti, le attività aziendali, nel cui ambito possano essere potenzialmente commessi i reati di cui al medesimo Decreto.

In proposito, si ricorda che le fasi principali in cui si articola un sistema di gestione dei rischi finalizzato alla costruzione del Modello Organizzativo sono identificate come segue dalle previsioni del Decreto:

a) "identificazione dei rischi", i.e. analisi del contesto aziendale per evidenziare in quale area/settore di attività e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati nel Decreto;
b) "progettazione del sistema di controllo" (c.d. protocolli per la programmazione della formazione ed attuazione delle decisione dell'ente), i.e. valutazione del sistema esistente all'interno dell'ente e suo eventuale adeguamento, per renderlo idoneo a contrastare efficacemente i rischi identificanti, cioè per ridurre i rischi a un "livello accettabile", avendo riguardo *i)* alla probabilità di accadimento dell'evento e *ii)* all'impatto dell'evento stesso.

Nel rispetto di tali requisiti, i modelli di organizzazione e gestione possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative di categoria e giudicati idonei dal Ministero della Giustizia.

TeamSystem ha costruito il proprio Modello organizzativo sulla base della metodologia e dei criteri indicati dalle "*Linee Guida di Confindustria per la costruzione dei modelli di organizzazione gestione e controllo ex D.lgs. 231/2001*" ("**Linee Guida Confindustria**") del 7 marzo 2002, successivamente aggiornate, da ultimo, nel mese di marzo 2014, con l'approvazione del Ministero della Giustizia (cfr. Nota Ministero della Giustizia 21 luglio 2014).

Si precisa, tuttavia, che le indicazioni – a carattere necessariamente generale e standardizzato – dettate dalla Linee Guida Confindustria sono state talora integrate o disattese laddove ritenuto necessario al fine di adeguarne i principi alla peculiarità e concretezza della realtà aziendale.

XVII. Passi operativi e metodologia applicata

Si riportano brevemente di seguito le fasi di attività in cui si è articolato il processo seguito per la predisposizione e l'aggiornamento del Modello, precisando che l'avvio di tali attività è stato preceduto da una fase di presentazione al *management* della Società al fine di garantirne un effettivo coinvolgimento nelle attività necessarie all'adozione del Modello.

Le attività propedeutiche in questione sono state svolte attraverso un'attività di *self-assessment* (condotta con il supporto di consulenti esterni) che ha avuto ad oggetto l'esame della documentazione aziendale (organigrammi, deleghe e procure societarie, *policy*, procedure, linee guida e regolamenti interni adottati dalla Società, etc.), dei processi e della prassi aziendali anche a mezzo di colloqui individuali con il personale della Società.

L'attività di verifica è stata condotta, inoltre, attraverso l'analisi di ulteriori elementi rilevanti ai fini del processo di identificazione dei rischi e di valutazione delle aree/attività maggiormente esposte alla commissione di reati, tra cui:

- la specifica "storia" della Società, tra cui, in particolare, la presenza di eventuali procedimenti di carattere penale, amministrativo o anche civile che abbia interessato la Società con riguardo alle attività a rischio;

- le dimensioni della Società e del Gruppo cui la medesima appartiene (in relazione a dati quali fatturato, numero di dipendenti);
- i mercati e gli ambiti territoriali in cui la Società opera;
- la struttura organizzativa;
- la preesistenza di un'etica aziendale;
- la qualità del clima aziendale esistente all'interno dell'organizzazione;
- la collaborazione tra i responsabili delle varie funzioni;
- la comunicazione tra il *management* e i lavoratori;
- il grado di separazione delle funzioni;
- le prassi che influenzano lo svolgimento dei vari processi.

Peraltro, nel processo di identificazione e valutazione dei rischi qui condotto si sono tenuti in considerazione anche elementi esterni alla struttura organizzativa delle Società, qualora ritenuti idonei ad incidere sui fattori di rischio esistenti, quali eventuali rischi riscontrati in aziende appartenenti al medesimo settore di attività.

L'attività di *risk assessment* è stata condotta in via propedeutica all'aggiornamento del Modello Organizzativo e successivamente aggiornata, da ultimo nel corso del 2018-2019. Le attività svolte sono descritte nel documento "*Risk Self Assessment*", che viene conservato agli atti della società.

XVIII. Reati rilevanti per TeamSystem S.p.A.

Sulla base dell'analisi condotta, anche in fase di aggiornamento del Modello, i reati potenzialmente realizzabili nel contesto aziendale di TeamSystem S.p.A. sono i seguenti:

- 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 (artt. 24);
- delitti informatici e trattamento illecito di dati (art. 24-bis);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis);
- reati societari (art. 25-ter);
- delitti contro la personalità individuale (art. 25-quinquies);
- abusi di mercato (art. 25-sexies);
- omicidio colposo o lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- delitti in materia di violazione del diritto d'autore (art. 25-novies);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies);
- reati ambientali (art. 25-undecies);
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies);
- reati transnazionali (art. 10, L. 146/2006);

- reati tributari (art. 25-quinquiesdecies).

Il rischio di commissione dei reati di cui agli artt. 25 *quater* "Delitti con finalità di terrorismo o di eversione dell'ordine democratico", 25 *quarter* "Pratiche di mutilazione degli organi genitali femminili", 25 *terdecies* "Razzismo e Xenofobia" è stato ritenuto estremamente remoto in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperto dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società, che vincola tutti i suoi destinatari alla più rigorosa osservanza delle leggi e delle normative ad essa applicabili.

Con particolare riguardo ai reati di cui all'art. 25 *bis* "Delitti contro l'industria e il commercio", la fattispecie di reato frode nell'esercizio del commercio si riferisce esclusivamente a beni mobili. Si è quindi provveduto a considerare i reati contro l'industria e il commercio potenzialmente non applicabili per la Società, tuttavia si precisa che la Società ha comunque provveduto ad implementato protocolli di controlli tali da mitigare il rischio di commissione di reati contro l'industria e il commercio.

Questa esclusione deriva dalle attività di mappatura delle attività a rischio reato come risultato di tutto il processo di analisi effettuato sia in fase preliminare sia in fase di interviste ed è stata condivisa con il Vertice aziendale.

Le principali aree di attività all'interno delle quali è stato riscontrato il rischio potenziale di commissione dei reati del Decreto sono quelle di seguito riportate (per un maggior dettaglio si faccia riferimento al documento di analisi delle aree aziendali e delle attività "a Rischio", i.e. Allegato "Matrice delle Aree ed Attività a Rischio-Reato"):

A. Gestione dei rapporti con la Pubblica Amministrazione ed enti certificatori.
B. Gestione delle visite ispettive.
C. Selezione, gestione ed assunzione del personale.
D. Gestione dei contenziosi giudiziali e stragiudiziali.
E. Gestione delle attività di amministrazione, finanza e controllo.
F. Gestione delle operazioni straordinarie.
G. Gestione dei sistemi informativi e della sicurezza informatica.
H. Approvvigionamento di beni e servizi.
I. Progettazione e commercializzazione di *software* applicativi per elaboratori.
J. Gestione delle *partnership.*
K. Gestione della Salute e Sicurezza sul Lavoro.
L. Gestione adempimenti ambientali
M. Attività promozionali, marketing e relazioni con il mercato.

XIX. Principi di controllo interno generali e specifici

Il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di: esplicita formalizzazione delle norme comportamentali; chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna direzione e alle diverse qualifiche e ruoli professionali; precisa descrizione delle attività di controllo e loro tracciabilità; adeguata segregazione di ruoli operativi e ruoli di controllo.

In particolare, devono essere perseguiti i seguenti principi generali di controllo interno:

Norme comportamentali

- Esistenza di un Codice Etico che descriva regole comportamentali di carattere generale a presidio delle attività svolte.

Definizioni di ruoli e responsabilità

- La regolamentazione interna deve declinare ruoli e responsabilità delle unità organizzative a tutti i livelli, descrivendo in maniera omogenea, le attività proprie di ciascuna struttura;
- tale regolamentazione deve essere resa disponibile e conosciuta all'interno dell'organizzazione.

Procedure e norme interne

- Le attività sensibili devono essere regolamentate, in modo coerente e congruo, attraverso gli strumenti normativi aziendali, così che in ogni momento si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato;
- deve essere individuato e formalizzato un Responsabile per ciascuna attività sensibile, tipicamente coincidente con il responsabile della struttura organizzativa competente per la gestione dell'attività stessa.

Segregazione dei compiti

- All'interno di ogni processo aziendale rilevante, devono essere separate le funzioni o i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla;
- non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno.

Poteri autorizzativi e di firma

- Deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando l'impresa e manifestando la sua volontà;
- i poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- le procure devono essere coerenti con il sistema interno delle deleghe;
- sono previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni;
- il sistema di deleghe deve identificare, tra l'altro:
    - i requisiti e le competenze professionali che il delegato deve possedere in ragione dello specifico ambito di operatività della delega;
    - l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguente assunzione degli obblighi conferiti;
    - le modalità operativa di gestione degli impegni di spesa;
- le deleghe sono attribuite secondo i principi di:
    - autonomia decisionale e finanziaria del delegato;
    - idoneità tecnico-professionale del delegato;
    - disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- nell'ambito delle procedure o di altra regolamentazione interna devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità);
- la documentazione afferente alle attività sensibili deve essere adeguatamente formalizzata e riportare la data di compilazione, presa visione del documento e la firma riconoscibile del compilatore/supervisore; la stessa deve essere archiviata in luogo idoneo alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e

smarrimenti;

- devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate;
- il responsabile dell'attività deve produrre e mantenere adeguati report di monitoraggio che contengano evidenza dei controlli effettuati e di eventuali anomalie;
- deve essere prevista, laddove possibile, l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile e ai soggetti che vi partecipano. Il sistema deve prevedere l'impossibilità di modifica (non tracciata) delle registrazioni;
- i documenti riguardanti l'attività della Società, ed in particolare i documenti o la documentazione informatica riguardanti attività sensibili sono archiviati e conservati, a cura della direzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;
- l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a loro delegato, al Collegio Sindacale od organo equivalente o ad altri organi di controllo interno, alla società di revisione eventualmente nominata e all'Organismo di Vigilanza.

Prestazione di servizi infragruppo

La prestazione di beni o servizi da parte delle società del Gruppo TeamSystem, con particolare riferimento a beni o servizi che possono riguardare aree a rischio reato e relative Attività Sensibili, devono avvenire nel rispetto dei seguenti principi:

- obbligo che tutti i contratti infragruppo siano stipulati per iscritto;
- obbligo da parte della società prestatrice di attestare la veridicità e la completezza della documentazione prodotta e delle informazioni comunicate alla Società in forza di obblighi di legge;
- impegno da parte della società prestatrice di rispettare, per la durata del contratto, i principi fondamentali del Codice di Comportamento e del Modello, nonché le disposizioni del D.Lgs. 231/2001 e di operare in linea con essi.

XX. Aggiornamento del Modello

L'adozione e l'efficace attuazione del Modello sono - per espressa previsione legislativa - una responsabilità rimessa al Consiglio di Amministrazione. Ne deriva che il potere di adottare eventuali aggiornamenti del Modello compete, dunque, al Consiglio di Amministrazione, che lo eserciterà mediante delibera con le modalità previste per la sua adozione.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal Decreto.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione.

A tal riguardo, si ricorda che il Decreto espressamente prevede la necessità di aggiornare il Modello al fine di renderlo costantemente "ritagliato" sulle specifiche esigenze dell'ente e della sua concreta operatività. Gli interventi di adeguamento e/o aggiornamento del Modello potranno rendersi ad esempio necessari in occasione di:

- innovazioni normative;

- violazioni del Modello e/o rilievi emersi nel corso di verifiche sull'efficacia del medesimo (che potranno anche essere desunti da esperienze riguardanti altre società);
- modifiche della struttura organizzativa dell'ente, anche derivanti da operazioni di finanza straordinaria ovvero da mutamenti nella strategia d'impresa derivanti da nuovi campi di attività intrapresi.

XXI. Informazione e formazione del personale

È obiettivo generale di TeamSystem S.p.A. garantire verso tutti i destinatari del Modello una corretta conoscenza e divulgazione delle regole di condotta ivi contenute. Tutto il personale, nonché i soggetti apicali, i consulenti, i partner ed i collaboratori esterni sono tenuti ad avere piena conoscenza sia degli obiettivi di correttezza e trasparenza che si intendono perseguire con il Modello, sia delle modalità attraverso le quali la Società intende perseguirli.

In tale contesto:

— ***Comunicazione iniziale e informazione***: l'adozione del Modello viene comunicata ai dipendenti, ai responsabili di funzione e ai dirigenti attraverso:

- l'invio di una comunicazione a firma dell'Amministratore Delegato a tutto il personale sui contenuti del Decreto, l'importanza dell'effettiva attuazione del Modello, le modalità di informazione previste dalla Società;
- la messa a disposizione del Modello nelle modalità più idonee, tra cui: i) la messa a disposizione di copia dello stesso nelle sessioni di formazione; ii) idonea diffusione sul sito intranet e internet; iii) l'affissione in bacheca; iv) l'invio dello stesso in formato elettronico;

— ***Formazione***: È inoltre prevista un'adeguata attività formativa del personale e dei collaboratori della Società sui contenuti del Decreto e del Modello***.*** Tale attività formativa viene articolata nelle seguenti fasi:

- attività di formazione generale: i.e. un'attività di formazione generica volta ad informare i destinatari sulle prescrizioni del Decreto e sui contenuti del Modello adottato dalla Società;
- attività di formazione specifica: i.e. un'attività di formazione specifica di coloro che operano nelle aree a rischio reato volta ad informare i destinatari, in particolare sui a) i rischi specifici a cui è esposta l'area nella quale operano e b) i principi di condotta e le procedure aziendali che essi devono seguire nello svolgimento della loro attività. La formazione, in particolare, dovrà riguardare, oltre al Codice Etico, anche gli altri strumenti di prevenzione quali le procedure, le policies, i flussi di informazione e gli altri protocolli adottati dalla Società in relazione alle diverse attività a rischio.

Al fine di garantire un'adeguata attività formativa ai destinatari è inoltre necessario che la formazione sia ripetuta i) in occasione di cambiamenti di mansioni che incidano sui comportamenti rilevanti ai fini del Modello (formazione anche di tipo individuale sotto forma di istruzioni specifiche e personali); ii) in relazione all'introduzione di modifiche sostanziali al Modello o, anche prima, all'insorgere di nuovi eventi particolarmente significativi rispetto al Modello (formazione collettiva).

L'attività formativa è organizzata tenendo in considerazione, nei contenuti e nelle modalità di erogazione, della qualifica dei destinatari e del livello di rischio dell'area in cui operano e potrà, dunque, prevedere diversi livelli di approfondimento, con particolare attenzione verso quei dipendenti che operano nelle aree a rischio.

I corsi di formazione, le relative tempistiche e le modalità attuative saranno definite dal responsabile delle Risorse Umane sentito il parere dell'OdV, che provvederanno anche a definire le forme di controllo sulla frequenza ai corsi e la qualità del contenuto dei programmi di formazione. In particolare, la formazione potrà essere realizzata mediante sessioni in aula, in modalità e-learning e con la consegna di materiale informativo volto ad illustrare i contenuti del Decreto, il Modello Organizzativo e le sue componenti (ivi incluso il Codice Etico ed il Sistema Disciplinare). A tale proposito, le relative attività formative dovranno essere previste e concretamente effettuate sia al momento dell'assunzione, sia in occasione di eventuali mutamenti di mansioni, nonché a seguito di aggiornamenti e/o modifiche del Modello.

La partecipazione ai corsi di formazione sul Modello è obbligatoria; la mancata partecipazione alle attività di formazione costituisce una violazione del Modello stesso e può dar luogo all'applicazione di sanzioni disciplinari. La Società ha implementato un sistema di monitoraggio dell'effettiva fruizione dei corsi formativi,

con particolare riferimento al corso 231, da parte dei destinatari al fine di identificare eventuali destinatari che non hanno svolto il corso e predisporre gli opportuni interventi correttivi.

Sono previste, inoltre, forme di verifica dell'apprendimento da parte dei destinatari della formazione mediante questionari di comprensione dei concetti esposti durante le sessioni formative, con obbligo di ripetizione della formazione in caso di esito non soddisfacente.

Il sistema di informazione e formazione è costantemente verificato e, ove occorra, modificato dall'OdV, in collaborazione con la Direzione Risorse Umane o di altri responsabili di funzione.

L'attività di informazione e formazione effettivamente svolta dovrà essere opportunamente documentata e la relativa documentazione sarà conservata dalla Direzione delle Risorse Umane.

5 Organismo di Vigilanza

I. L'Organismo di Vigilanza e i suoi requisiti

Al fine di garantire alla Società l'esimente dalla responsabilità amministrativa in conformità a quanto previsto dall'art. 6 del Decreto, è necessaria l'individuazione e la costituzione da parte della Società di un Organismo di Vigilanza fornito dell'autorità e dei poteri necessari per vigilare, in assoluta autonomia, sul funzionamento e sull'osservanza del Modello, nonché di curarne il relativo aggiornamento, proponendone le modifiche o integrazioni ritenute opportune al Consiglio di Amministrazione della Società.

I componenti dell'Organismo di Vigilanza della Società (di seguito anche "**OdV**") sono scelti tra soggetti in possesso dei requisiti di autonomia, indipendenza e professionalità richiesti dal Decreto per svolgere tale ruolo.

Il Decreto 231/01 non fornisce indicazioni alcuna circa la composizione dell'OdV; pertanto, la scelta tra una sua composizione mono soggettiva o plurisoggettiva e l'individuazione dei suoi componenti - interni o esterni all'ente - devono tenere conto - come suggerito dalle Linee Guida di Confindustria e come confermato dalla giurisprudenza in materia - delle finalità perseguite dalla legge in uno con la tipologia di società nella quale l'OdV andrà ad operare, dovendo esso assicurare il profilo di effettività dei controlli in relazione alla dimensione e alla complessità organizzativa dell'ente.

In base a tali indicazioni, l'OdV deve possedere le seguenti principali caratteristiche:

Autonomia ed indipendenza

I requisiti di autonomia ed indipendenza che l'OdV deve necessariamente possedere, affinché la Società possa andare esente da responsabilità, si riferiscono in particolare alla funzionalità dello stesso OdV. La posizione dell'OdV nell'ambito delle Società dovrà cioè assicurare l'autonomia dell'iniziativa di controllo da ogni interferenza o condizionamento proveniente dalla Società e dai suoi organi dirigenti. Tali requisiti sono assicurati tramite la collocazione dell'OdV in una posizione di vertice in seno all'organizzazione aziendale, senza attribuzione, formale o anche solo in via di fatto, di alcun ruolo esecutivo che possa renderlo partecipe di decisioni ed attività operative della Società, che altrimenti lo priverebbero della necessaria obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

I requisiti di autonomia e indipendenza oltre che a riferirsi all'OdV nel suo complesso debbono anche riferirsi ai suoi componenti singolarmente considerati: in caso di OdV a composizione plurisoggettiva, nei quali alcuni componenti siano esterni e altri interni, non essendo esigibile dai componenti di provenienza interna una totale indipendenza dalle Società, il grado di indipendenza dell'OdV dovrà essere valutato nella sua globalità.

Al fine di garantire l'effettiva sussistenza dei requisiti sopra descritti, è opportuno che i membri dell'OdV posseggano alcuni requisiti soggettivi formali che garantiscano ulteriormente la loro autonomia e indipendenza come previsto dalle Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231 approvate il 7 marzo 2002 ed aggiornate il marzo 2014 (ad esempio onorabilità, assenza di conflitti di interesse con gli organi sociali e con il vertice aziendale etc.).

Professionalità

I componenti l'OdV debbono possedere, così come specificato anche in talune pronunce giurisprudenziali, apposite competenze tecniche, onde poter provvedere efficacemente all'espletamento dei propri compiti ispettivi e di controllo. Trattasi di tecniche di tipo specialistico, proprie di chi svolge attività ispettiva, consulenziale e giuridica.

Con riferimento all'attività ispettiva e di analisi del sistema di controllo, è opportuno che i membri dell'OdV abbiano esperienza, ad esempio, nelle tecniche di analisi e valutazione dei rischi, nelle misure per il loro contenimento, nel *flow-charting* di procedure e processi per l'individuazione dei punti di debolezza, nelle tecniche di intervista e di elaborazione dei questionari.

Si ricorda in ogni caso che l'OdV, al fine di adempiere ai propri compiti, può utilizzare, oltre alle competenze specifiche dei singoli membri, anche risorse aziendali interne o consulenti esterni.

Continuità di azione

Al fine di garantire l'efficace e costante attuazione del Modello Organizzativo, l'OdV deve garantire continuità nell'esercizio delle sue funzioni, che non deve essere intesa come "presenza continua", ma come effettività e frequenza del controllo.

La definizione degli aspetti attinenti alla continuità d'azione dell'OdV, quali la calendarizzazione dell'attività, la verbalizzazione delle riunioni, la frequenza e la modalità delle riunioni, è rimessa allo stesso Organismo, il quale, nell'esercizio della propria facoltà di autoregolamentazione, dovrà disciplinare il proprio funzionamento interno. A tal proposito è opportuno che l'OdV stesso formuli un regolamento delle proprie attività (es. modalità di convocazione delle riunioni, documentazione dell'attività, etc.).

Si precisa, infine, che la Legge n. 183 del 2011 (c.d. Legge di Stabilità per il 2012), ha espressamente previsto la possibilità per le società di capitali di affidare al Collegio Sindacale le funzioni di Organismo di Vigilanza (art. 6, comma 4-bis del Decreto). Pertanto, la Società ha la facoltà di optare per questa forma di organizzazione dell'OdV, anche in considerazione delle esigenze di razionalizzazione complessiva del sistema dei controlli adottato.

Libero accesso

Libero accesso a tutte le informazioni aziendali che ritiene rilevanti.

Autonomia di spesa

Autonomia di spesa per quanto attiene allo svolgimento delle sue funzioni fintanto che le stesse sono necessarie per l'attuazione ed il funzionamento del Modello.

II. Composizione dell'Organismo di Vigilanza, nomina, revoca, cause di ineleggibilità e di decadenza dei suoi membri

Il numero e la qualifica dei componenti dell'Organismo di Vigilanza è stabilito dal Consiglio di Amministrazione, che provvede alla nomina dell'OdV e del suo Presidente mediante apposita delibera consiliare motivata, che dia atto della sussistenza dei requisiti di autonomia, indipendenza e professionalità che i membri dell'OdV devono possedere.

I componenti dell'OdV rimangono in carica per tre anni e sono rieleggibili.

I componenti dell'Organismo di Vigilanza, nell'esercitare le proprie funzioni, devono mantenere i necessari requisiti di autonomia e indipendenza richiesti dal Decreto: essi devono pertanto comunicare immediatamente al Consiglio di Amministrazione e allo stesso Organismo di Vigilanza l'insorgere di eventuali situazioni che non consentano di conservare il rispetto di tali requisiti.

I membri dell'Organismo di Vigilanza designati restano in carica per tutta la durata del mandato ricevuto, a prescindere dalla modifica di composizione del Consiglio di Amministrazione che li ha nominati, a meno che il rinnovo del Consiglio di Amministrazione dipenda dalla commissione di uno dei Reati contemplati nel Decreto: in tal caso il neo eletto organo amministrativo provvederà a costituire un nuovo Organismo di Vigilanza.

Non possono essere eletti alla carica di componenti dell'Organismo di Vigilanza e, se eletti, decadono automaticamente dall'ufficio:

- coloro che si trovano nelle condizioni previste dall'articolo 2382 del Codice Civile (interdizione, inabilitazione, fallimento, condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'incapacità ad esercitare uffici direttivi);
- il coniuge, i parenti e gli affini entro il quarto grado degli amministratori non-indipendenti della Società; il coniuge, i parenti e gli affini entro il quarto grado degli amministratori non-indipendenti delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo;
- coloro che sono stati condannati con sentenza ancorché non definitiva (ivi compresa quella pronunciata ex art. 444 c.p.p.):
    - alla reclusione per un tempo non inferiore a un anno: i) per uno dei delitti previsti dal RD n. 267/1942; ii) per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, dei mercati e dei valori mobiliari e di strumenti di pagamento; iii) per un delitto contro la

pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica o in materia tributaria;

- alla reclusione per un tempo non inferiore a due anni per qualunque delitto non colposo;
- per uno o più reati tra quelli previsti e richiamati dal Decreto, a prescindere dal tipo di condanna inflitta;
- per un reato che importi la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

- coloro nei cui confronti sia stata applicata una delle misure di prevenzione previste dall'art. 3 della legge 19 marzo 1990, n. 55 e sue successive modifiche.

In caso di nomina di un componente esterno, lo stesso non dovrà avere rapporti commerciali con la Società che possano determinare l'insorgere di conflitti di interesse.

Fatte salve le ipotesi di decadenza automatica, i componenti dell'OdV non possono essere revocati dal Consiglio di Amministrazione se non per giusta causa.

Rappresentano ipotesi di giusta causa di revoca:

- una sentenza di condanna della Società ai sensi del Decreto, o una sentenza di patteggiamento, ove risulti dagli atti l'"omessa o insufficiente vigilanza" da parte dell'OdV secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- il mancato riserbo relativamente alle informazioni di cui vengano a conoscenza nell'espletamento dell'incarico;
- la mancata partecipazione a più di due riunioni dell'OdV consecutive senza giustificato motivo.

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

L'OdV si intende decaduto se vengono a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, il Consiglio di Amministrazione provvede a nominare di nuovo tutti i componenti dell'OdV.

Ove sussistano gravi ragioni di convenienza, il Consiglio di Amministrazione procederà a disporre la sospensione dalle funzioni di uno o tutti i membri dell'OdV, provvedendo tempestivamente alla nomina di un nuovo membro o dell'intero Organismo *ad interim*.

III. L'Organismo di Vigilanza di Team System

Sulla base dei presupposti e delle considerazioni sopra riportate, contestualmente all'adozione del proprio Modello Organizzativo, la Società ha provveduto all'istituzione dell'Organismo di Vigilanza (OdV) e alla nomina dei suoi componenti. Nella sua attuale composizione, l'OdV è stato nominato con delibera del 15 luglio 2019.

La scelta è stata quella di affidare le funzioni di Organismo di Vigilanza ad un organismo a composizione collegiale, con un numero di membri pari a tre, individuati in tre professionisti esterni, uno dei quali con funzione di Presidente dell'OdV.

In considerazione delle dimensioni e delle caratteristiche dell'organizzazione aziendale e della complessità dei compiti che l'OdV è chiamato a svolgere, la composizione sopra descritta pare la più idonea a garantire l'autonomia, la professionalità, nonché la continuità d'azione che devono contraddistinguere l'operato di detto Organismo.

La scelta di nominare tre componenti esterni (individuando tra di essi il Presidente dell'OdV) risponde, invero, all'esigenza di rafforzare i requisiti di autonomia e indipendenza dell'Organismo, oltre che di professionalità dello stesso. Più precisamente, quale Presidente dell'OdV è stato individuato un professionista esterno, esercente la professione di avvocato, specializzato in diritto delle nuove tecnologie e dotato di competenze di carattere penalistico, oltre che specificatamente in materia di compliance al D.lgs. 231/2001.

Tutti i componenti hanno maturato esperienze professionali quali componenti di Organismi di vigilanza in società operanti a livello nazionale ed internazionale.

IV. Compiti, Poteri e funzioni dell'Organismo di Vigilanza

L'Organismo di Vigilanza svolge le funzioni di vigilanza e controllo previste dal Decreto e dal Modello.

L'Organismo di Vigilanza dispone di autonomi poteri di iniziativa e di controllo nell'ambito della Società tali da consentire l'efficace esercizio delle funzioni previste dal Decreto e dal Modello.

Per ogni esigenza necessaria al corretto svolgimento dei propri compiti, l'Organismo di Vigilanza dispone di adeguate risorse finanziarie che vengono assegnate allo stesso sulla base di *un budget* di spesa approvato dal Consiglio di Amministrazione, su proposta dell'OdV stesso. Le attività poste in essere dall'OdV non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che il Consiglio di Amministrazione è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto sul Consiglio di Amministrazione grava in ultima istanza la responsabilità del funzionamento e dell'efficacia del Modello.

L'OdV è chiamato a svolgere le seguenti attività:

a) Attività di verifica e vigilanza:

- vigilanza sull'osservanza del Modello;
- verifica dell'effettiva adeguatezza e capacità del Modello di prevenire la commissione degli illeciti previsti dal Decreto;
- vigilanza sulla corretta applicazione del Sistema Disciplinare da parte delle funzioni aziendali allo stesso preposte;

b) Aggiornamento del Modello

- valutazione del mantenimento nel tempo della solidità e funzionalità del Modello, verificando che la Società curi l'aggiornamento del Modello e proponendo, se necessario, al Consiglio di Amministrazione o alle funzioni aziendali eventualmente competenti, l'adeguamento dello stesso, al fine di migliorarne l'adeguatezza e l'efficacia, in relazione alle mutate condizioni aziendali e/o legislative;
- attività di follow-up, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

c) Informazione e formazione

- promozione della diffusione nel contesto aziendale della conoscenza e della comprensione del Modello;
- promozione e monitoraggio delle iniziative, ivi inclusi i corsi e le comunicazioni, volte a favorire un'adeguata conoscenza del Modello da parte di tutti i Destinatari;
- valutazione e risposta alle richieste di chiarimento provenienti dalle funzioni aziendali ovvero dagli organi amministrativi e di controllo, qualora connesse e/o collegate al Modello.

d) Reporting da e verso l'OdV

- attuazione, in conformità al Modello, di un efficace flusso informativo nei confronti degli organi sociali competenti in merito all'efficacia e all'osservanza del Modello;
- verifica del puntuale adempimento, da parte dei soggetti interessati, di tutte le attività di
- *reporting* inerenti al Modello;
- esame e valutazione di tutte le informazioni e/o le segnalazioni ricevute in relazione al Modello, ivi incluso per ciò che attiene le eventuali violazioni dello stesso;
- in caso di controlli da parte di soggetti istituzionali, ivi inclusa la Pubblica Autorità, previsione del

necessario supporto informativo agli organi ispettivi.

Nell'ambito delle attività sopra enunciate, l'OdV provvederà ai seguenti adempimenti:

- promuovere la diffusione e la verifica nel contesto aziendale della conoscenza e della comprensione dei principi delineati nel Modello;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree e le attività a rischio individuate, effettuando, qualora lo ritenga necessario ai fini dell'espletamento delle proprie funzioni, anche controlli non preventivamente programmati (c.d. "controlli a sorpresa");
- verificare e controllare la regolare tenuta ed efficacia di tutta la documentazione inerente le attività/operazioni individuate nel Modello;
- verificare periodicamente le procure e le deleghe interne in vigore, raccomandando le necessarie modifiche nel caso in cui le stesse non siano più coerenti con le responsabilità organizzative e gestionali;
- istituire (facendone richiesta alle competenti funzioni aziendali) specifici canali informativi "dedicati" (es. indirizzi di posta elettronica), diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- valutare periodicamente l'adeguatezza del Modello rispetto alle disposizioni ed ai principi regolatori del Decreto e le corrispondenti esigenze di aggiornamento;
- valutare periodicamente l'adeguatezza del flusso informativo e adottare le eventuali misure correttive;
- comunicare e relazionare periodicamente al Consiglio di Amministrazione in ordine alle attività svolte, alle segnalazioni ricevute, agli interventi correttivi e migliorativi del Modello e al loro stato di realizzazione.

Ai fini dello svolgimento degli adempimenti ad esso affidati, all'OdV sono attribuiti i poteri e le facoltà qui di seguito indicati:

- emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'Organismo;
- accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'OdV, ivi inclusi i libri societari di cui all'art. 2421 del cod. civ.;
- richiedere la collaborazione, anche in via continuativa, di strutture interne o ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
- disporre che i soggetti destinatari della richiesta forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- condurre le indagini interne necessarie per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- richiedere alle funzioni aziendali preposte e delegate alla gestione dei procedimenti disciplinari e all'irrogazione delle sanzioni informazioni, dati e/o notizie utili a vigilare sulla corretta applicazione del sistema disciplinare;
- richiedere, attraverso i canali e le persone appropriate, la riunione del Consiglio di Amministrazione per affrontare questioni urgenti;
- accedere alla documentazione elaborata dal Collegio Sindacale;

- richiedere ai responsabili di funzione di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza.

Considerate le funzioni dell'Organismo di Vigilanza ed i contenuti professionali specifici da esse richieste, nello svolgimento dell'attività di vigilanza e controllo, l'Organismo di Vigilanza può avvalersi del supporto delle altre funzioni interne alla Società che, di volta in volta, si rendessero necessarie per un'efficace svolgimento delle attività di verifica.

L'Organismo di Vigilanza, qualora lo ritenga opportuno e/o nei casi in cui si richiedano a questa funzione attività che necessitino di specializzazioni professionali non presenti al suo interno, né all'interno della Società stessa, avrà la facoltà di avvalersi delle specifiche capacità professionali di consulenti esterni ai quali delegare predefiniti ambiti di indagine e le operazioni tecniche necessarie per lo svolgimento della funzione di controllo. I consulenti dovranno, in ogni caso, sempre riferire i risultati del loro operato all'Organismo di Vigilanza.

V. Reporting dell'Organismo di Vigilanza

L'OdV riferisce in merito all'attuazione del Modello ed all'attività svolta secondo le seguenti linee di *reporting:*

a) su base annuale, al Consiglio d'Amministrazione, al quale dovrà essere trasmessa una relazione scritta avente in particolare ad oggetto:

- l'attività complessivamente svolta nel periodo di riferimento;
- una *review* delle segnalazioni ricevute e delle azioni intraprese dall'OdV o da altri soggetti,
- ivi incluse le sanzioni disciplinari (connesse con comportamenti rilevanti ai fini del Decreto) eventualmente irrogate dai soggetti competenti;
- le criticità emerse in relazione al Modello ed i necessari e/o opportuni interventi correttivi e migliorativi del Modello e al loro stato di realizzazione;
- l'individuazione, con cadenza annuale, del piano di attività per l'anno successivo;

b) su base continuativa e qualora ne ravvisi la necessità, all'Amministratore Delegato e al Consiglio di Amministrazione. In particolare, l'OdV dovrà:

- segnalare tempestivamente al Consiglio di Amministrazione qualsiasi violazione del Modello che sia ritenuta fondata dall'Organismo stesso, di cui sia venuto a conoscenza per segnalazione da parte dei dipendenti o dallo stesso accertata;
- segnalare tempestivamente al Consiglio di Amministrazione rilevate carenze organizzative o procedurali idonee a determinare il concreto pericolo di commissione di reati rilevanti ai fini del Decreto;
- segnalare all'Amministratore Delegato o al Consiglio di Amministrazione l'esistenza di modifiche normative particolarmente rilevanti ai fini dell'attuazione ed efficacia del Modello;
- trasmettere tempestivamente al Consiglio d'Amministrazione ogni altra informazione rilevante al fine del corretto svolgimento delle funzioni proprie dell'Organismo stesso, nonché al fine del corretto adempimento delle disposizioni di cui al Decreto.

L'OdV di TeamSystem, potrà essere convocato in qualsiasi momento dai suddetti organi o potrà a sua volta presentare richiesta in tal senso, per riferire in merito al funzionamento del Modello o a situazioni specifiche.

VI. Whistleblowing

Il Decreto Legislativo 10 marzo 2023, n. 24, recante "*Attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*" ha profondamente modificato la normativa in materia di Whistleblowing modificando l'art. 6, comma 2 bis del D.lgs. 231/2001 che prevede: «I *modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento*

europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e).».

La Legge sul *whistleblowing* introduce nell'ordinamento giuridico italiano un apparato di norme volto a migliorare l'efficacia degli strumenti di contrasto ai comportamenti illeciti, contrari sia a norme nazionali che dell'Unione Europea,, nonché a tutelare con maggiore intensità gli autori delle segnalazioni incentivando il ricorso allo strumento della denuncia di condotte illecite o di violazioni dei modelli di organizzazione, gestione e controllo, gravando il datore di lavoro dell'onere di dimostrare - in occasione di controversie legate all'irrogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti o alla sottoposizione del segnalante ad altra misura organizzativa successiva alla presentazione della segnalazione avente effetti negativi, diretti o indiretti, sulla condizione di lavoro - che tali misure risultino fondate su ragioni estranee alla segnalazione stessa (c.d. "inversione dell'onere della prova a favore del segnalante").

La Società ha istituito un apposito Sistema di Whistleblowing ed elaborato una disposizione ad hoc, la "*Politica gestione delle segnalazioni (Whistleblowing)*".

Tale strumento rappresenta un ulteriore meccanismo di monitoraggio della conformità alle normative in vigore e si applica alle segnalazioni che hanno ad oggetto violazioni pertinenti l'attività della Società e qualsiasi altra violazione delle norme che possa avere impatto (ad esempio sanzionatorio, patrimoniale, reputazionale, etc.).

Sono stati istituiti al riguardo canali di comunicazione idonei a garantire la riservatezza dell'identità del segnalante e la corretta gestione delle relative segnalazioni (ancorché anonime). In particolare, le segnalazioni di violazioni possono essere effettuate una piattaforma internet ("Piattaforma di Whistleblowing") appositamente creata disponibile all'indirizzo https://whistleblowing.teamsystem.com. Tale piattaforma mette a disposizione un apposito modello per l'effettuazione della segnalazione. Inoltre, registrando la segnalazione sul portale, viene assegnato un codice identificativo univoco ("key code"), che potrà essere utilizzato dal segnalante per "dialogare" con chi riceve la segnalazione e per essere informato sullo stato di lavorazione della segnalazione inviata.

In caso di segnalazioni interne che abbiano ad oggetto atti/fatti che possano costituire una violazione di norme disciplinanti l'attività della Società, ma che contestualmente possano avere rilevanza anche ai fini del D. Lgs. 231/2001, il Comitato "Whistleblowing" è incaricato di inviare apposita informativa all'Organismo di Vigilanza, avendo cura di tutelare la riservatezza del segnalante e dei soggetti tutelati dalla normativa, qualora sia necessario valutare l'eventuale avvio di ulteriori approfondimenti ai sensi del D. Lgs. 231/2001.

Per qualsiasi ulteriore dettaglio si rinvia alla normativa interna indicata.

VII. Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza, secondo quanto previsto dai protocolli adottati e nelle singole Parti Speciali del Modello.

Per ciascuna "area a rischio reato" saranno identificati uno o più "Responsabili Interni" che dovranno, tra l'altro, fornire all'OdV i flussi informativi secondo le modalità e con la frequenza definite in uno specifico "Protocollo dei flussi informativi", che costituisce parte integrante del presente Modello Organizzativo. Si ritiene, infatti, opportuno che la gestione dei flussi informativi verso l'Organismo di Vigilanza sia regolata da una specifica procedura, opportunamente diffusa e comunicata a tutti i destinatari, allo scopo di assicurare una maggiore efficacia nell'attuazione dei flussi informativi. Anche nel caso in cui, nel periodo selezionato, non vi siano state segnalazioni significative da comunicare all'OdV, allo stesso dovrà essere inviata una segnalazione "negativa".

Sono stati inoltre istituiti precisi obblighi gravanti sugli organi sociali e sul personale di TeamSystem in particolare:

- gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello;
- i Destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni delle prescrizioni del Modello o fattispecie di reato.

Le segnalazioni di cui sopra possono essere effettuate in forma scritta al seguente indirizzo di posta elettronica:

organismodiviglianza@teamsystem.com

ovvero, a mezzo di posta, all'Organismo di Vigilanza presso la sede della Società, corrente in:

TeamSystem S.p.A., Att.ne Organo di Vigilanza, via Sandro Pertini, 88 61121 – Pesaro

indicando sulla busta la dicitura "PERSONALE E STRETTAMENTE RISERVATO – DA NON APRIRE" in modo tale da garantirne la riservatezza.

Fermo restando quanto precede, verranno esaminate, purché sufficientemente precise e circostanziate, anche le segnalazioni indirizzate o, comunque, portate a conoscenza dei singoli membri dell'Organismo di Vigilanza, i quali provvederanno a condividere le informazioni ricevute con gli altri componenti dell'Organismo.

L'Organismo di Vigilanza agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti, comunque, salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede in linea da quanto previsto dalla policy in materia.

Laddove la segnalazione rilevante ai sensi del D.lgs. 24/2023 venga ricevuta dall'OdV al proprio indirizzo e-mail e/o cartaceamente, questi provvede entro 7 giorni dalla ricezione ad inoltrarla al Comitato Whistleblowing ed a informare il Segnalante. Il Comitato gestirà la segnalazione secondo quanto previsto dalla policy, informandone l'OdV ed in collaborazione con lo stesso nel caso di violazione rilevanti ai sensi del D.lgs. 231/2001, fermo restando quanto previsto dal D.lgs. 24/2023 in materia di tutela della riservatezza.

In ogni caso, i flussi informativi trasmessi all'Organismo di Vigilanza devono necessariamente prevedere le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento della Società o di soggetti apicali, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- attività di controllo svolte dai responsabili di altre direzioni aziendali dalle quali siano emersi fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o del Modello;
- modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
- procedimenti disciplinari avviati in relazione alla violazione del Codice Etico o del Modello Organizzativo e relativi esiti (anche in caso di archiviazione);
- segnalazione di infortuni gravi (in ogni caso qualsiasi infortunio con prognosi superiore ai 40 giorni) occorsi a dipendenti, addetti alla manutenzione, appaltatori e/o collaboratori presenti nei luoghi di lavoro della Società;
- eventuali ordini ricevuti dal superiore e ritenuti in contrasto con la legge, la normativa interna o il Modello;
- elenco finanziamenti pubblici chiesti/ottenuti nel periodo con lo stato di avanzamento del progetto; Verbali di ispezioni, visite e accertamenti da parte di organi pubblici di vigilanza ed eventuali sanzioni;
- contenziosi attivi e passivi in corso e, alla loro conclusione, i relativi esiti;

- eventuali richieste o offerte di denaro, doni o di altre utilità provenienti da, pubblici ufficiali o incaricati di pubblico servizio;
- eventuali scostamenti significativi di *budget* o anomalie di spesa non debitamente motivati, emersi dalle richieste di autorizzazione nella fase di consuntivazione del Controllo di Gestione;
- eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- eventuali segnalazioni, non tempestivamente riscontrate dalle funzioni competenti, concernenti sia carenze o inadeguatezze dei luoghi, delle attrezzature di lavoro, ovvero dei dispositivi di protezione messi a disposizione della Società, sia ogni altra situazione di pericolo connesso alla tutela dell'ambiente e della salute e sicurezza sul lavoro.

VIII. Invio di informazioni sulle modifiche dell'organizzazione aziendale all'Organismo di Vigilanza

Al fine di agevolare le attività di verifica e monitoraggio svolte dall'Organismo di Vigilanza con riferimento alle attività a rischio di commissione reato ed alla luce dell'assetto organizzativo adottato dalla Società, i Responsabili Interni individuati in seno all'organizzazione aziendale quali referenti dell'Organismo di Vigilanza devono trasmettere all'Organismo di Vigilanza, ciascuno con riferimento alle attività svolte direttamente o comunque sotto la propria responsabilità, con la periodicità e secondo le modalità individuate dalla Società, anche su proposta dell'OdV, le seguenti informazioni:

- notizie relative a cambiamenti organizzativi (ad esempio, mutamenti negli organigrammi societari, revisioni delle procedure esistenti o adozioni di nuove procedure o *policies*, ecc.);
- gli aggiornamenti e i mutamenti del sistema delle deleghe e dei poteri;
- le eventuali comunicazioni del soggetto incaricato della revisione legale dei conti riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni;
- copia dei verbali delle riunioni del Consiglio di Amministrazione e del Collegio Sindacale da cui emergano modifiche organizzative, criticità nell'attuazione del sistema di controllo interno o comunque fatti o notizie rilevanti ai fini della corretta attuazione o della necessità di aggiornamento del Modello Organizzativo;
- copia delle eventuali comunicazioni effettuate all'Autorità di Vigilanza (ad es: Autorità Garante per la Concorrenza e del mercato, Autorità garante per la protezione dei dati personali, etc.);
- ogni altra informazione che l'Organismo di Vigilanza dovesse richiedere l'esercizio delle sue funzioni.

IX. Il regolamento dell'Organismo di Vigilanza

L'OdV ha la responsabilità di redigere un proprio regolamento interno volto a disciplinare gli aspetti e le modalità concrete dell'esercizio della propria azione, ivi incluso per ciò che attiene al relativo sistema organizzativo e di funzionamento.

X. Archiviazione delle informazioni

Di tutte le richieste, le consultazioni e le riunioni tra l'OdV e le altre funzioni aziendali, l'Organismo di Vigilanza ha l'obbligo di predisporre idonea evidenza documentale ovvero apposito verbale di riunione. Tale documentazione verrà custodita sotto la responsabilità dell'Organismo di Vigilanza medesimo.

Ogni informazione, segnalazione, report previsti dal presente Modello sono conservati dall'Organismo di Vigilanza in un apposito e riservato archivio informatico e/o cartaceo in conformità alla normativa sulla protezione dei dati personali.

6 Sistema sanzionatorio

I. Principi generali

L'effettività del Modello è legata anche all'adeguatezza del sistema sanzionatorio per la violazione delle regole di condotta e, in generale, delle procedure e dei regolamenti interni.

Il Sistema Disciplinare opera nel rispetto delle norme vigenti, ivi incluse quelle della contrattazione collettiva, ha natura eminentemente interna a TeamSystem S.p.A., non sostitutivo, ma preventivo e complementare rispetto alle norme di legge o di regolamento vigenti, nonché integrativo delle altre norme di carattere intra-aziendale.

L'applicazione delle misure sanzionatorie stabilite dal Modello non sostituisce eventuali ulteriori sanzioni di altra natura (quali a titolo esemplificativo, penale, amministrativa, civile e tributaria) che possano derivare dal medesimo fatto di reato.

Per quanto non espressamente previsto nel Sistema Disciplinare, troveranno applicazione le norme di legge e di regolamento ed, in particolare, le previsioni di cui all'art. 7 della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) nonché le previsioni della contrattazione collettiva e dei regolamenti aziendali applicabili.

L'applicazione di sanzioni disciplinari per violazione delle regole di condotta ed inosservanza delle disposizioni aziendali è indipendente dal giudizio penale e dal suo esito, in quanto tali normative sono assunte dall'azienda in piena autonomia a prescindere dal carattere di illecito penale che la condotta possa configurare.

La sanzione sarà commisurata alla gravità dell'infrazione e alla eventuale reiterazione della stessa; della recidività si terrà altresì conto anche ai fini della comminazione di una eventuale sanzione espulsiva.

Una non corretta interpretazione dei principi e delle regole stabiliti dal Modello potrà costituire esimente soltanto nei casi di comportamenti di buona fede in cui i vincoli posti dal Modello dovessero eccedere i limiti di approfondimento richiesti ad una persona di buona diligenza.

Sono sanzionabili:

- le violazioni di procedure interne previste dal presente Modello o l'adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello sia che espongano sia che non espongano la società ad una situazione oggettiva di rischio di commissione di uno dei Reati ex D. Lgs. 231/2001;
- l'adozione di comportamenti in violazione alle prescrizioni del presente Modello e diretti in modo univoco al compimento di uno o più Reati;
- l'adozione di comportamenti in violazione delle prescrizioni del presente Modello, tale da determinare la concreta o potenziale applicazione a carico della Società di sanzioni previste dal D.Lgs. 231/2001;

la violazione delle disposizioni previste dal D.lgs. 24/2023 in materia di Whistleblowing e relative procedure interne

Le sanzioni, di natura disciplinare e contrattuale, e l'eventuale richiesta di risarcimento danni, verranno commisurate anche al livello di responsabilità ed autonomia del Dipendente, ovvero al ruolo e all'intensità del vincolo fiduciario connesso all'incarico conferito agli Amministratori, Società di Service (intendendosi le società terze con le quali la Società intrattiene rapporti contrattuali).

Il sistema sanzionatorio è soggetto a costante verifica e valutazione da parte dell'Organo di Vigilanza e dell'Amministratore Delegato e del Responsabile Risorse Umane, rimanendo quest'ultimi responsabili della concreta applicazione delle misure disciplinari nei confronti del Dipendente qui delineate, su eventuale segnalazione dell'Organo di Vigilanza e sentito il superiore gerarchico dell'autore della condotta censurata.

Il sistema sanzionatorio di natura disciplinare troverà applicazione anche nei confronti dell'Organo di Vigilanza o di quei soggetti, Dipendenti o Amministratori, che, per negligenza ed imperizia, non abbiano individuato e conseguentemente eliminato i comportamenti posti in violazione del Modello.

II. Destinatari e apparato sanzionatorio e/o risolutivo

Aspetto essenziale per l'effettività del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al

Decreto, e, in generale, delle procedure interne previste dal Modello stesso.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.

— Sanzioni per i lavoratori dipendenti

Ai comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono applicabili – fatta eccezione per i richiami verbali – le procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e le norme pattizie di cui al Contratto Collettivo Nazionale di Lavoro del Commercio a cui si rimanda.

In particolare, in caso di (a) violazione delle disposizioni del Modello, delle sue procedure interne (ad esempio il mancato rispetto delle procedure, la mancata comunicazione delle informazioni richieste all'Organismo di Vigilanza, il mancato svolgimento dei controlli, etc.), del Codice Etico, del Decreto o di qualsivoglia altra disposizione penale in esso inclusa o (b) mancato rispetto delle disposizioni di cui al Modello nello svolgimento di attività in aree "a rischio" o (c) danneggiamento della Società o l'aver causato una situazione oggettiva di pericolo per i beni della stessa (gli "Illeciti Disciplinari") saranno applicabili i seguenti provvedimenti disciplinari per i Dipendenti:

- richiamo verbale;
- ammonizione scritta;
- multa in misura non eccedente l'importo di 4 ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di 10 giorni;
- licenziamento.

— Contestazione dell'infrazione e giustificazioni del dipendente

La contestazione dell'infrazione al lavoratore deve essere fatta in forma scritta con l'indicazione specifica dei fatti costitutivi dell'infrazione. Il provvedimento disciplinare non potrà essere emanato se non sono trascorsi 5 giorni da tale contestazione, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni. Se il provvedimento non verrà emanato entro i 5 giorni successivi, tali giustificazioni si riterranno accolte. Al contrario, se le giustificazioni del lavoratore non saranno accolte, il provvedimento disciplinare dovrà essere emanato entro i 6 giorni dalla contestazione dell'illecito anche nel caso in cui il dipendente non presenti alcuna giustificazione.

Nel caso in cui l'infrazione contestata sia di gravità tale da comportare la sanzione massima, ovvero il licenziamento, il lavoratore potrà essere sospeso cautelativamente dalla prestazione lavorativa fino al momento della comminazione del provvedimento, fermo restando il suo diritto a ricevere la retribuzione per il periodo considerato.

La comminazione del provvedimento dovrà essere motivata e comunicata in forma scritta. I provvedimenti disciplinari diversi dal licenziamento potranno essere impugnati in sede sindacale secondo le norme previste dai CCNL di riferimento. Non si terrà conto delle sanzioni trascorsi 2 anni dalla loro applicazione.

— Sanzioni disciplinari

1. Nel provvedimento della "Ammonizione scritta":

il lavoratore dipendente che per la prima volta violi le procedure interne previste dal presente Modello (ad esempio che non osservi le procedure prescritte, ometta di dare comunicazione all'OdV delle informazioni prescritte, etc.) o adotti, nell'espletamento della propria attività, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una non esecuzione degli ordini impartiti dall'azienda sia in forma scritta che verbale.

2. Nel provvedimento della "Multa":

il lavoratore dipendente che violi più volte le procedure interne previste dal presente Modello o adotti,

nell'espletamento della propria attività, un comportamento più volte non conforme alle prescrizioni del Modello stesso, prima ancora che dette mancanze siano state singolarmente accertate e contestate, dovendosi ravvisare in tali comportamenti la ripetuta non esecuzione degli ordini impartiti dall'azienda sia in forma scritta che verbale; tenuto conto della gravità del comportamento e delle mansioni svolte dal lavoratore, potrà essere comminata la sanzione della multa anche in caso di prima mancanza. L'ammontare della multa erogata non può essere superiore a quanto previsto dai CCNL di riferimento.

3. Nel provvedimento della "Sospensione dal lavoro e dalla retribuzione":

il lavoratore dipendente che incorra in recidiva in violazioni già punite con la multa nei sei mesi precedenti; tenuto conto della gravità del comportamento e delle mansioni svolte dal lavoratore, potrà essere comminata la sanzione della multa anche in caso di prima mancanza qualora il lavoratore dipendente, nel violare le procedure interne previste dal presente Modello o adottando nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, nonché compiendo atti contrari all'interesse della Società, arrechi danno alla Società o la esponga a una situazione oggettiva di pericolo alla integrità dei beni dell'azienda, dovendosi ravvisare in tali comportamenti la non esecuzione degli ordini impartiti dall'azienda sia in forma scritta che verbale. Il periodo di sospensione dalla retribuzione non può essere superiore a quanto previsto dai CCNL di riferimento.

4. Nel provvedimento del "Licenziamento senza preavviso":

il lavoratore che adotti, nell'espletamento della propria attività un comportamento palesemente in violazione delle prescrizioni del presente Modello e tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto, dovendosi ravvisare in tale comportamento una condotta tale da provocare alla azienda grave nocumento morale e/o materiale nonché da costituire atti implicanti dolo o colpa grave con danno per l'azienda.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, saranno applicate, ai sensi di quanto previsto dalla Società, in relazione:

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- al comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- alle mansioni del lavoratore;
- alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- alle altre particolari circostanze che accompagnano la violazione disciplinare.

— Sanzioni nei confronti dei dirigenti

Nel caso in cui i dirigenti commettano un Illecito Disciplinare, si provvederà ad applicare nei confronti dei responsabili le seguenti misure in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti industriali:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel richiamo scritto all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave violazione – o ripetute violazioni - di una o più prescrizioni del Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del licenziamento con preavviso;
- laddove la violazione di una o più prescrizioni del Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il lavoratore incorre nel provvedimento del licenziamento senza preavviso.

— Misure nei confronti degli Amministratori e dei Sindaci

In caso di Illeciti Disciplinari commessi da Amministratori o da Sindaci della Società, l'OdV informerà l'intero Consiglio di Amministrazione e il Collegio Sindacale della stessa i quali provvederanno ad assumere le

opportune iniziative previste dalla vigente normativa, coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, revoca per giusta causa, ecc.).

— Misure nei confronti di Collaboratori, Partner e Consulenti

I Collaboratori esterni, fornitori, i Consulenti e i Partner della Società, con particolare riferimento a soggetti coinvolti nella prestazione di attività, forniture o servizi che interessano attività a rischio ai sensi del Modello, vengono informati sull'adozione del Modello e dell'esigenza della Società, che il loro comportamento sia conforme ai principi di condotta ivi stabiliti.

La Società valuta le modalità (ad es. diffusione sul sito Intranet), a seconda delle diverse tipologie di collaboratori esterni e partner, con cui provvedere ad informare tali soggetti sulle politiche e sulle procedure seguite dalla Società in virtù dell'adozione del Modello e per assicurarsi che tali soggetti si attengono al rispetto di tali principi, prevedendo altresì l'adozione di idonee clausole contrattuali che obblighino tali soggetti ad ottemperare alle disposizioni del Modello medesimo, sotto pena di risoluzione automatica del rapporto contrattuale e fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società.

III. Misure nei confronti dei destinatari delle segnalazioni ("*Whistleblowing*")

La Società, in caso di violazione delle disposizioni normative in materia di *whistleblowing* al fine di tutelare l'identità del segnalante e lo stesso da eventuali atti di ritorsione o discriminazione, potrà applicare in relazione al destinatario della segnalazione le seguenti sanzioni:

Sono, pertanto, irrogabili sanzioni nei confronti di qualsivoglia soggetto:

- violi le misure in materia di tutela della riservatezza del segnalante e/o delle procedure emanate dalla Società ai sensi del D.Lgs. 24/2023 o ostacoli la segnalazione;
- compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del Segnalante e degli altri soggetti tutelati dalla normativa per motivi collegati, direttamente o indirettamente, alla segnalazione effettuata;
- effettui segnalazioni, poste in essere con dolo o colpa grave, che siano o si rivelino infondate In particolare quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele previste dalla legge non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare.
- **Esponenti aziendali (dipendenti, dirigenti, amministratori, organi di controllo)**

In caso di violazione delle disposizioni sopra previste in materia di Whistleblowing da parte di un esponente aziendale (dipendente, dirigente, amministratore) saranno applicate le sanzioni sopra previste, graduate a seconda della gravità del fatto.

- ***Organismo di Vigilanza***

In caso di violazione del presente Modello o di violazione della riservatezza dell'identità del segnalante da parte di uno o più membri dell'OdV, gli altri membri dell'Organismo informeranno immediatamente l'Organo Amministrativo: tale Organo, previa contestazione della violazione e concessione degli adeguati strumenti di difesa, prenderà gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico ai membri dell'OdV che hanno posto in essere la violazione e la conseguente nomina di nuovi membri in sostituzione degli stessi ovvero la revoca dell'incarico all'intero organo e la conseguente nomina di un nuovo OdV.

- ***Membri del Comitato Segnalazioni***

In caso di violazione del presente Modello o di violazione della riservatezza dell'identità del segnalante da parte dei membri del Comitato quali destinatari delle segnalazioni, verrà informato immediatamente l'Amministratore Delegato che, previa contestazione della violazione e concessione degli adeguati strumenti di difesa, prenderà gli opportuni provvedimenti in considerazione delle violazioni e della condotta posta in essere oltre ad eventuali ulteriori previsioni di legge.

IV. Misure nei confronti dei soggetti esterni aventi rapporti contrattuali / commerciali

I rapporti con terze parti sono regolati da adeguati contratti che devono prevedere clausole di rispetto dei principi fondamentali del Modello e del Codice Etico da parte di tali soggetti esterni. In particolare, il mancato rispetto degli stessi deve comportare la risoluzione per giusta causa dei medesimi rapporti, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti per la Società.

L'adozione - da parte di *partner* commerciali, fornitori, consulenti e collaboratori esterni, comunque denominati, o altri soggetti aventi rapporti contrattuali con la Società - di comportamenti in contrasto con i principi ed e i protocolli indicati nel presente Modello sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali che saranno inserite nei relativi contratti.

La violazione grave o reiterata dei principi contenuti nel Modello e nel Codice Etico della Società sarà considerata inadempimento degli obblighi contrattuali e potrà dar luogo alla risoluzione del contratto da parte di TeamSystem.

PARTE SPECIALE

La parte speciale del Modello di Organizzazione, Gestione e Controllo *ex* D. Lgs. 231/01 si sviluppa partendo dalle analisi effettuate all'interno della scheda descrittiva denominata Matrice delle aree a rischio reato.

Per ogni "Area a Rischio" individuata durante le attività di mappatura sono analizzati nella parte speciale del Modello:

Attività sensibili: sono riportate le attività collegate all'area sensibile nello svolgimento delle quali è stato riscontrato un rischio potenziale di commissione di alcuni reati richiamati dal Decreto.

Reati potenziali: sono identificati i reati potenziali associabili alle attività sensibili.

Esempi di possibili modalità di realizzazione del reato: sono descritte, a titolo esemplificativo e non esaustivo, le possibili condotte illecite del reato e le relative finalità a favore della Società.

Sistema di controllo a presidio del rischio reato: al fine di mitigare il rischio di commissione dei reati nell'ambito delle attività sensibili sono stati identificati i comportamenti e le misure di prevenzione.

Come già visto in precedenza nella parte generale, oltre ai controlli di seguito descritti, per ogni area di attività a rischio sono presenti elementi di mitigazione del rischio che valgono in maniera trasversale su tutte le aree e i processi aziendali:

- sistemi di governo;
- struttura gerarchico-funzionale (organigramma aziendale);
- sistema di deleghe e procure;
- principi generali di comportamento riconosciuti e applicati (Codice Etico);
- corpo procedurale e documentale della Società nel suo insieme;
- sistema disciplinare e sanzionatorio efficace e diffuso;
- comunicazione e formazione;
- sistemi informativi integrati e orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi utilizzati a supporto delle attività operative connesse al *business*;
- corretta archiviazione di tutta la documentazione presso gli uffici preposti.

Il sistema di controllo coinvolge ogni settore dell'attività svolta dalla Società attraverso la distinzione dei compiti operativi da quelli di controllo, riducendo ragionevolmente la possibile realizzazione dei reati. Le Sezioni di seguito riportate si riferiscono ai comportamenti posti in essere dai Destinatari del presente Modello, così come definiti nella Parte Generale, coinvolti nelle Aree di attività "a rischio". Obiettivo della regolamentazione è che tutti i soggetti interessati tengano comportamenti conformi a quanto prescritto dalla legge, dal Modello, dai suoi strumenti di attuazione, dal Codice Etico nonché dal corpo procedurale e documentale della Società, al fine di prevenire la commissione dei reati contemplati nel D. Lgs. 231/01.

SEZIONE A - Gestione dei rapporti con la Pubblica Amministrazione ed enti certificatori

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione dei rapporti con la Pubblica Amministrazione ed enti certificatori, ed in particolare alle attività sensibili:

- Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (es. Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni);
- Gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (Autorità Garante della Concorrenza e del mercato, Ufficio Brevetti, Garante Privacy, Antitrust, ANAC, ecc.) e gli enti certificatori (es. ISO) e gestione delle comunicazioni e delle informazioni a esse dirette;
- Gestione dei rapporti con gli enti pubblici competenti per l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione, sia per la richiesta che per la rendicontazione;
- Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. Registro delle imprese presso le Camere di Commercio competenti).

Reati applicabili

In relazione alle attività sensibili relative all'are di rischio gestione dei rapporti con la Pubblica Amministrazione ed enti certificatori di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, intrattengano rapporti con pubblici ufficiali, incaricati di pubblico servizio o, più in generale, con rappresentanti della Pubblica Amministrazione (di seguito, "Rappresentanti della Pubblica Amministrazione"), anche di Stati esteri.

In particolare, nei confronti della Pubblica Amministrazione è fatto espresso divieto di:

a) esibire documenti e dati incompleti e/o comunicare dati falsi e alterati;

b) sottrarre o omettere l'esibizione di documenti veri;

c) omettere informazioni dovute;

d) indurre taluno in errore utilizzando artifici o raggiri ai fini di conseguire un ingiusto profitto in danno dello Stato, di altro ente pubblico o dell'Unione Europea. In particolare, si raccomanda il rispetto della legge e della corretta pratica commerciale a fronte di trattative, concessioni, licenze, ecc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;

e) assecondare la condotta induttiva di un pubblico ufficiale o di un incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità;

f) procurare indebitamente qualsiasi altro tipo di profitto (licenze, autorizzazioni, sgravi di oneri, anche previdenziali, ecc.) con mezzi che costituiscano artifici o raggiri (per esempio invio di documentazione non veritiera);

g) destinare a uso diverso un finanziamento ottenuto dallo Stato, o da altro ente pubblico o dall'Unione Europea.

Inoltre, gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati:

a) nel rispetto delle norme di legge vigenti;

b) garantendo i principi di trasparenza, onestà e correttezza, al fine di non compromettere l'integrità e la reputazione della Società;

c) con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere;

d) evitando e, comunque, segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse.

Infine, nei confronti degli enti certificatori è fatto divieto di:

a) esibire documenti e dati incompleti e/o comunicare dati falsi e alterati;

b) sottrarre o omettere l'esibizione di documenti veri;

c) omettere informazioni dovute;

d) ricercare o instaurare illecitamente relazioni personali di favore, influenza o ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto con gli enti certificatori o con la Pubblica Amministrazione.

Protocolli specifici di prevenzione

a) Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (es. Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni).

Per l'attività sensibile Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (es. Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni) i protocolli prevedono che:

- i rapporti con i Rappresentanti della Pubblica Amministrazione devono essere gestiti esclusivamente dai soggetti aziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- tutti i contratti che hanno come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;

- tutta la documentazione deve essere autorizzata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste
- gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati evitando e, comunque, segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- nel caso di esternalizzazione dei rapporti con la PA sia sempre contrattualizzato il rapporto con lo studio di consulenza o con i professionisti esterni e sia sempre prevista una clausola che preveda l'accettazione di clausole 231 da parte della controparte;

b) Gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (Autorità Garante della Concorrenza e del mercato, Ufficio Brevetti, Garante Privacy, Antitrust, ANAC, ecc.) e gli enti certificatori (es. ISO) e gestione delle comunicazioni e delle informazioni a esse dirette.

Per l'attività sensibile gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (Autorità Garante della Concorrenza e del mercato, Ufficio Brevetti, Garante Privacy, Antitrust, ANAC, ecc.) e gli enti certificatori (es. ISO) e gestione delle comunicazioni e delle informazioni a esse dirette i protocolli prevedono che:

- le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono essere gestiti esclusivamente dai soggetti aziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- tutti i contratti che hanno come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;
- tutta la documentazione deve essere autorizzata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- qualora i pubblici funzionari redigano un verbale in occasione degli accertamenti condotti presso la Società, il responsabile di direzione coinvolto ha l'obbligo di firmare questi verbali e di mantenerne copia nei propri uffici;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati evitando e, comunque, segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;

- nel caso di esternalizzazione dei rapporti con la PA sia sempre contrattualizzato il rapporto con lo studio di consulenza o con i professionisti esterni e sia sempre prevista una clausola che preveda l'accettazione di clausole 231 da parte della controparte.

c) Gestione dei rapporti con gli enti pubblici competenti per l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione, sia per la richiesta che per la rendicontazione.

Per l'attività sensibile gestione dei rapporti con gli enti pubblici competenti per l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione, sia per la richiesta che per la rendicontazione, i protocolli prevedono che:

- le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono gestiti esclusivamente dai soggetti aziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- deve essere adottata una procedura o altro strumento normativo aziendale che regolamenti l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione, sia per la richiesta che per la rendicontazione;
- tutti i contratti che hanno come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;
- tutta la documentazione deve essere autorizzata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- qualora i pubblici funzionari redigano un verbale in occasione degli accertamenti condotti presso la Società, il responsabile di direzione coinvolto, o il suo delegato, ha l'obbligo di firmare questi verbali e di mantenerne copia nei propri uffici;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- si effettui, in conformità con le procedure aziendali che regolamentano questa attività, una valutazione preliminare del possesso dei requisiti previsti per poter accedere ai contributi/finanziamenti, nonché continuo monitoraggio al fine di verificare il mantenimento degli stessi;
- vi sia una chiara definizione dei ruoli e delle responsabilità operative con riferimento alla gestione dei finanziamenti pubblici;
- si effettui un continuo monitoraggio, supportato da evidenze formali, circa il corretto utilizzo dei fondi/finanziamenti ricevuti rispetto agli scopi cui erano destinati;
- gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati evitando e, comunque, segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;

- nel caso di esternalizzazione dei rapporti con la PA sia sempre contrattualizzato il rapporto con lo studio di consulenza o con i professionisti esterni e sia sempre prevista una clausola che preveda l'accettazione di clausole 231 da parte della controparte.

d) Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. Registro delle imprese presso le Camere di Commercio competenti).

Per l'attività sensibile gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. Registro delle imprese presso le Camere di Commercio competenti), i protocolli prevedono che:

- le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono gestiti esclusivamente dai soggetti aziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- tutti i contratti che hanno come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;
- tutta la documentazione deve essere autorizzata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- sia effettuato un monitoraggio della normativa di riferimento e si provveda all'archiviazione della documentazione;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- nel caso di esternalizzazione dei rapporti con la PA sia sempre contrattualizzato il rapporto con lo studio di consulenza o con i professionisti esterni e sia sempre prevista una clausola che preveda l'accettazione di clausole 231 da parte della controparte.

Area di rischio: Gestione dei rapporti con la Pubblica Amministrazione ed enti certificatori

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/CP	RIC	IT	IND *	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	
Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (es. Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni).	✔														PA - Personale della Società, nell'interesse della stessa, organizza meeting per avvicinare pubblici funzionari al fine di ottenere indebitamente commesse.
Gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (Autorità Garante della Concorrenza e del mercato, Ufficio Brevetti, Garante Privacy, Antitrust, ANAC, ecc.) e gli enti certificatori (es. ISO) e gestione delle comunicazioni e delle informazioni a esse dirette.	✔	✔													PA - La Società condiziona indebitamente la Pubblica Amministrazione al fine di ottenere l'adozione di provvedimenti compiacenti o l'omissione di misure che comportino sanzioni o il riconoscimento di responsabilità in capo alla Società. SOC/CP – La Società condiziona indebitamente un ente certificatore al fine di ottenere una certificazione senza adottare i provvedimenti necessari all'ottenimento.
Gestione dei rapporti con gli enti pubblici competenti per l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione, sia per la richiesta che per la rendicontazione.	✔														PA - La Società potrebbe offrire o promettere vantaggi a pubblici funzionari in vista dell'attribuzione di contributi/finanziamenti pubblici o agevolati, ovvero dell'impegno a non rilevare difformità esistenti nell'impiego del finanziamento concesso, o ancora la corresponsione di denaro o altra utilità da parte della Società a ciò indotta dal pubblico ufficiale infedele.
Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. Registro delle imprese presso le Camere di Commercio competenti).	✔														PA - La Società condiziona indebitamente il funzionario della Pubblica Amministrazione al fine di ottenere o l'omissione di misure che comportino sanzioni o il riconoscimento di responsabilità in capo alla Società in occasione di visite ispettive.
Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti e degli enti certificatori in occasione di visite ispettive	✔	✔													PA - La Società condiziona indebitamente la Pubblica Amministrazione al fine di ottenere l'omissione di misure che comportino sanzioni durante visite ispettive. SOC/CP – La Società condiziona indebitamente un ente certificatore al fine di omettere la mancanza di un requisito necessario alla certificazione durante una visita ispettiva.

SEZIONE B - Gestione delle visite ispettive

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione delle visite ispettive, ed in particolare all'attività sensibile:

- Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti e degli enti certificatori in occasione di visite ispettive.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione delle visite ispettive di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, intrattengano rapporti con pubblici ufficiali, incaricati di pubblico servizio o, più in generale, con rappresentanti della Pubblica Amministrazione (di seguito, "Rappresentanti della Pubblica Amministrazione"), anche di Stati esteri.

In particolare, nei confronti della Pubblica Amministrazione è fatto espresso divieto di:

a) esibire documenti e dati incompleti e/o comunicare dati falsi e alterati;
b) sottrarre o omettere l'esibizione di documenti veri;
c) omettere informazioni dovute;
d) ricercare o instaurare illecitamente relazioni personali di favore, influenza o ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto con la Pubblica Amministrazione;
e) indurre taluno in errore utilizzando artifici o raggiri ai fini di conseguire un ingiusto profitto in danno dello Stato, di altro ente pubblico o dell'Unione Europea. In particolare, si raccomanda il rispetto della legge e della corretta pratica commerciale a fronte di trattative, concessioni, licenze, ecc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;
f) assecondare la condotta induttiva di un pubblico ufficiale o di un incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Protocolli specifici di prevenzione

a) Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti e degli enti certificatori in occasione di visite ispettive.

Per l'attività sensibile Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti e degli enti certificatori in occasione di visite ispettive i protocolli prevedono che:

- le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono gestiti esclusivamente dai soggetti aziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- tutti i contratti che hanno come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;
- i funzionari della Pubblica Amministrazione devono essere accompagnati durante le verifiche ispettive da almeno due rappresentanti di TeamSystem;
- tutta la documentazione deve essere verificata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- la gestione dei rapporti con i pubblici funzionari in caso di visite ispettive è totalmente nella responsabilità del responsabile di direzione competente, o da un suo delegato, che gestisce i sopralluoghi dalla fase di accoglimento alla firma del verbale di accertamento;
- nel caso di esternalizzazione dei rapporti con la PA sia sempre contrattualizzato il rapporto con lo studio di consulenza o con i professionisti esterni e sia sempre prevista una clausola che preveda l'accettazione di clausole 231 da parte della controparte;
- qualora i pubblici funzionari redigano un verbale in occasione degli accertamenti condotti presso la Società, il responsabile di direzione coinvolto, o il suo delegato, ha l'obbligo di firmare questi verbali e di mantenerne copia nei propri uffici;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati evitando e, comunque, segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- sia effettuato un monitoraggio della normativa di riferimento e si provveda all'archiviazione della documentazione.

Area di rischio: Gestione delle visite ispettive

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	
Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti e degli enti certificatori in occasione di visite ispettive.	✔	✔													PA - La Società corrompe un Pubblico Ufficiale al fine di ottenere l'omissione di misure che comportino sanzioni durante una visita ispettiva. SOC/CP – La Società potrebbe condizionare indebitamente un ente certificatore al fine di omettere la mancanza di un requisito necessario.

SEZIONE C – Selezione, gestione ed assunzione del personale

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio selezione, gestione ed assunzione del personale, ed in particolare alle attività sensibili:

- Gestione delle attività di selezione, assunzione e gestione del personale;
- Gestione dei benefit aziendali;
- Gestione del processo di valutazione della performance del personale e del sistema premiante.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio selezione, gestione ed assunzione del personale di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- delitti contro la personalità individuale (art. 25-quinquies);
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies);
- reati transnazionali (art. 10, L. 146/2006);
- reati tributari (art. 25-quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di selezionare, gestire e assumere il personale.

Inoltre, è fatto espresso divieto di:

a) assumere lavoratori stranieri privi di permesso di soggiorno;
b) assumere lavoratori il cui permesso sia scaduto – e per il quale non sia richiesto il rinnovo – revocato o annullato;
c) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

Protocolli specifici di prevenzione

a) Gestione delle attività di selezione, assunzione e gestione del personale.

Per l'attività sensibile Gestione delle attività di selezione, assunzione e gestione del personale i protocolli prevedono che:

- il processo di selezione del personale deve essere attivato solo in presenza di effettiva necessità e svolgersi secondo criteri di obiettività, imparzialità e rispondenza a interessi di organico;
- la lettera di impegno all'assunzione e il relativo contratto di assunzione devono essere firmate dal soggetto a ciò autorizzato secondo i poteri di firma;
- devono essere definite caratteristiche e requisiti per le figure professionali oggetto di assunzione;
- la Società può avvalersi esclusivamente di personale assunto in conformità alle tipologie contrattuali previste dalla normativa e dai contratti collettivi nazionali di lavoro applicabili;
- deve essere conservata evidenza documentale delle singole fasi del processo di selezione e assunzione del personale;
- la scelta dei dipendenti, dei consulenti e dei collaboratori deve avvenire a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile;
- nei limiti di quanto consentito dalle vigenti leggi in materia di protezione dei dati personali, devono essere preventivamente condotte verifiche circa il rischio di infiltrazione criminale nonché di possibili condizionamenti illeciti da parte di esponenti della pubblica Amministrazione o altri soggetti in grado di condizionare il processo di selezione;
- devono essere formalmente stabiliti ed efficacemente svolti controlli periodici e documentati sul calcolo e sul pagamento delle remunerazioni variabili;
- eventuali sistemi premianti ai dipendenti e collaboratori devono rispondere ad obiettivi realistici e coerenti con le mansioni, l'attività svolta e le responsabilità affidate;
- devono essere promosse e monitorate iniziative, ivi inclusi i corsi e le comunicazioni, volte a favorire un'adeguata conoscenza del Modello da parte di tutti i Destinatari;
- I passaggi di ruolo o di mansione e l'eventuale variazione di livello retributivo sono adeguatamente autorizzati ed avvengono secondo criteri obiettivi e documentati
- sia monitorata la validità dei permessi di soggiorno dei dipendenti non residenti in EU;
- sia svolta la valutazione comparativa di una rosa di almeno tre candidati, e qualora non sia possibile procedere alla valutazione di una pluralità di candidati, siano evidenziate le ragioni di tale impossibilità nel prospetto riepilogativo della selezione;
- siano presenti un numero variabile di *step* selettivi (minimo due colloqui) in funzione della posizione ricoperta e dell'area di appartenenza;
- i feedback degli incontri dei candidati siano tracciabili;
- sia verificato che al neo assunto siano stati consegnati i documenti previsti dalla normativa (con particolare riguardo alla normativa in materia di tutela dei rapporti di lavoro, salute, igiene e sicurezza sui luoghi di lavoro, ambiente, protezione dei dati personali e di responsabilità amministrativa degli enti) e dai regolamenti aziendali interni (tra cui il Codice Etico, il Codice di Condotta Anti-corruzione, il Modello Organizzativo, le procedure del sistema di gestione della sicurezza delle informazioni, ecc.);

- qualora ci si avvalga di società esterne per il processo di selezione (es. Società di *Head Hunting*), il rapporto con le stesse è formalizzato in appositi contratti, che prevedono l'accettazione delle clausole 231 e del Codice Etico;

b) Gestione dei benefit aziendali.

Per l'attività sensibile Gestione dei benefit aziendali i protocolli prevedono che:

- siano definiti i criteri e le modalità per l'utilizzo dei benefit aziendali;
- siano definiti i criteri e le modalità per l'assegnazione degli appartamenti;
- sia mantenuto un inventario aggiornato dei beni attribuiti agli assegnatari;
- siano definiti dei criteri e le modalità per la loro restituzione dei beni in caso di dimissioni o licenziamento o comunque di interruzione del rapporto di lavoro con la Società;
- la società riconosca ai dipendenti benefits di varia natura in relazione al ruolo ricoperto (es. autovettura, *tablet*, etc.) e ne definisca l'iter approvativo;
- siano definiti dei criteri e le modalità per l'assegnazione delle macchine ed e il loro utilizzo nonché il relativo iter di approvazione.

c) Gestione del processo di valutazione della performance del personale e del sistema premiante.

Per l'attività sensibile Gestione del processo di valutazione della performance del personale e del sistema premiante i protocolli prevedono che:

- siano definiti e documentati dei controlli periodici sul calcolo e sul pagamento delle remunerazioni variabili;
- Le componenti variabili di retribuzione sono liquidate solo a fronte di effettivo raggiungimento dei risultati fissati come obiettivo del sistema premiante, secondo un processo tracciabile e documentato
- eventuali sistemi premianti ai dipendenti e collaboratori devono rispondere ad obiettivi realistici e coerenti con le mansioni, l'attività svolta e le responsabilità affidate;
- gli obiettivi identificati siano verificati in sede di consuntivazione congiuntamente da Finance Strategic Planning, Direzione HR e dalla Direzione di riferimento;
- per assicurare che le Direzioni interessate, nella definizione degli obiettivi, non abbiano prefissato target di performance palesemente immotivati ed inarrivabili, vengono controllati il metodo di calcolo e la scala premiante attraverso l'analisi della scheda MBO compilata (con particolare riferimento alla sezione "Target, bonus e previsioni di costo").

Area di rischio: Selezione, gestione ed assunzione del personale

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione delle attività di selezione, assunzione e gestione del personale.	✔	✔					✔		✔			✔				PA - La Società strumentalizza ad interesse o vantaggio proprio, l'assunzione di risorse legate o gradite ad esponenti o enti della PA. SOC/CP - La Società assume risorse legate a rappresentanti della potenziale società cliente come contropartita per il compimento, da parte di questi, di comportamenti infedeli per la società cliente stessa. CRI/TSN - La Società assume risorse "gradite" a soggetti legati alla criminalità organizzata in cambio di favori da parte dell'associazione criminosa. IMP - La Società assume o si avvale di personale privo di regolare permesso di soggiorno anche attraverso l'utilizzo di Società Interinali. PI - La società utilizza personale senza rispettare quanto previsto dal CCNL.
Gestione dei benefit aziendali.	✔	✔													✔	PA - La Società utilizza benefit aziendali affinché attraverso l'utilizzo degli stessi con pubblici ufficiali o incaricati di pubblico servizio possa ottenere in cambio un beneficio per il business. SOC/CP - La Società fornisce al proprio personale benefit aziendali affinché attraverso l'utilizzo con terzi possa ottenere in cambio un beneficio per il business. RT - Nell'ambito della gestione amministrativa dei dipendenti, attraverso una determinazione artificiosa dei costi per il personale (ad es.: determinazione di componenti di retribuzione inesistenti rispetto alle prestazioni effettivamente conseguite, determinazione di voci di costo connesse a benefit aziendali non effettivamente erogati).
Gestione del processo di valutazione della performance del personale e del sistema premiante.	✔	✔														PA - Riconoscere incentivi e bonus al personale superiori agli importi dovuti, al fine di creare le disponibilità finanziarie con le quali perpetrare reati di corruzione. SOC/CP - Riconoscere incentivi e bonus al personale superiori agli importi dovuti, al fine di creare le disponibilità finanziarie con le quali perpetrare reati di corruzione verso privati.

SEZIONE D – Gestione dei contenziosi giudiziali e stragiudiziali

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione dei contenziosi giudiziali e stragiudiziali, ed in particolare alle attività sensibili:

- Gestione del contenzioso giudiziale e stragiudiziale e dei rapporti:

  - con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi con particolare riferimento alla nomina dei legali esterni;

  - con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

- Gestione delle transazioni fiscali

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione dei contenziosi giudiziali e stragiudiziali di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)
- reati tributari (art 25 quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire i contenziosi giudiziali e stragiudiziali.

Inoltre, è fatto espresso divieto di:

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

b) in particolare, a titolo meramente esemplificativo e non esaustivo, di elargire, promettere o dare denaro o altra utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni, ecc., ovvero a persone comunque indicate da codesti soggetti, nonché adottare comportamenti – anche a mezzo di soggetti terzi (es. professionisti esterni) - contrari alla legge e ai presidi aziendali, per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della Pubblica Amministrazione, quando questa

sia una parte nel contenzioso;

c) favorire indebitamente gli interessi della Società inducendo con violenza o minaccia, o, alternativamente, con offerta di danaro o altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;

d) offrire denaro, altra utilità o anche soltanto esercitare pressione e/o qualunque forma di condizionamento a coloro che dovessero risultare indagati/imputati (o persone informate sui fatti/testimone, test) in un procedimento penale connesso alla Società al fine di influenzarne il giudizio e/o limitarne la libertà di esprimere le proprie rappresentazioni dei fatti o di esercitare la facoltà di non rispondere accordata dalla legge, al fine di favorire gli interessi della Società o trarne un vantaggio per la medesima;

e) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

f) fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di cui alla presente Parte Speciale;

g) effettuare prestazioni in favore dei consulenti, dei *Partner* e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;

h) violare i principi di controllo previsti nella presente Parte Speciale;

i) prendere contatti con dipendenti coinvolti in procedimenti penali, allo scopo di indurli a rendere dichiarazioni atte ad evitare l'eventuale rischio di un coinvolgimento della società;

j) selezionare i soggetti autorizzati ad interloquire con i dipendenti coinvolti in procedimenti penali, e gli eventuali colloqui intercorsi verbalizzati;

k) presentare documenti, dati ed informazioni falsi nell'ambito di una transazione fiscale.

Protocolli specifici di prevenzione

a) Gestione del contenzioso giudiziale e stragiudiziale e dei rapporti:

- con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi con particolare riferimento alla nomina dei legali esterni;

- con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

Per l'attività sensibile Gestione del contenzioso giudiziale e stragiudiziale e dei rapporti con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari (nell'ambito delle cause di varia natura o dei relativi ricorsi, con particolare riferimento alla nomina dei legali esterni) o con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale, i protocolli prevedono che:

- siano fissati i limiti delle deleghe di spesa dei soggetti coinvolti nella gestione del contenzioso;
- siano stabiliti criteri di individuazione di legali esterni per la gestione dei contenziosi;
- l'articolazione del processo garantisca la segregazione funzionale tra i coloro che agiscono nell'ambito del processo di gestione del contenzioso:
- sia prevista la predisposizione di uno scadenzario che permetta di controllare l'intera attività esecutiva, con particolare riferimento al rispetto dei termini processuali previsti;
- sia garantita la tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate.
- sia sempre verificata la completa raccolta ed archiviazione della documentazione a supporto dell'attività consulenziale ricevuta (atti giudiziali, circolarizzazioni legali, consuntivi attività di

assistenza legale fornita, fatture/parcelle ricevute dai consulenti legali) in modo particolare quando di per sé non già sufficientemente tangibile (ad es. tramite la compilazione di una relazione scritta da parte del consulente).

b) Gestione delle vertenze/transazioni fiscali

Per la gestione dell'attività sensibile "Gestione delle vertenze/transazioni fiscali" i protocolli indicano la necessità di:

- garantire che i flussi comunicativi verso l'Autorità competente siano gestiti unicamente dalla Funzione a ciò preposta, che provvederà anche alla necessaria informativa in favore degli organi di controllo (Collegio Sindacale, Società di Revisione e Organismo di Vigilanza);
- richiedere la verifica con un consulente terzo in merito a eventuali implicazione fiscali derivanti dall'esecuzione di un'operazione avente carattere ordinario o straordinario, che comporti il trasferimento di assets della Società, soprattutto in presenza di un contenzioso tributario.

Area di rischio: Gestione dei contenziosi giudiziali e stragiudiziali

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione del contenzioso giudiziale e stragiudiziale e dei rapporti: - con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi con particolare riferimento alla nomina dei legali esterni; - con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale; - con la controparte per accordi stragiudiziali.	✔	✔			✔										✔	PA - La Società corrompe il Pubblico ufficiale al fine di ottenere un esito del giudizio favorevole per la Società. SOC/CP - La Società corrompe un rappresentante di una Società cliente al fine di ottenere un accordo transattivo vantaggioso. IND - La Società, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce un soggetto chiamato a rendere dichiarazioni davanti alla autorità giudiziaria, a non rendere dichiarazioni o a rendere dichiarazioni mendaci, al fine di influenzare l'esito del procedimento penale in favore della Società. RT - Nell'ambito della gestione delle controversie legali e di quelle correlate al lavoro, la Società rappresenta in modo non veritiero le spese legali sostenute, ostacolando la trasparente ricostruzione degli elementi passivi determinati in relazione a tali pendenze.
Gestione delle transazioni fiscali															✔	RT - Al fine di ottenere per sé o per altri un pagamento parziale dei tributi e accessori, la Società indica nella documentazione relativa alla transazione fiscale elementi attivi per un importo inferiore a quello effettivo o elementi passivi fittizi.

SEZIONE E – Gestione delle attività di amministrazione, finanza e controllo

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione delle attività di amministrazione, finanza e controllo, ed in particolare alle attività sensibili:

- Gestione della contabilità generale, con particolare riferimento alle attività di:
  - rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (es. gestione e registrazione contabile della fatturazione attiva);
  - verifica dati provenienti dai sistemi informativi alimentanti;
  - raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato.
- Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività:
  - autorizzazione e invio dei pagamenti;
  - inserimento / modifica delle coordinate bancarie del fornitore.
- Gestione dei rapporti con gli istituti finanziari;
- Gestione dei crediti;
- Rapporti con gli organi di controllo (es. Collegio Sindacale, Società di Revisione, ecc.) relativamente alle verifiche sulla gestione amministrativa/contabile, compresa la custodia e tenuta dei libri contabili e sociali;
- Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo;
- Rimborsi spese, anticipi e spese di rappresentanza;
- Gestione degli adempimenti fiscali;
- Archiviazione della documentazione contabile e fiscale.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione delle attività di amministrazione, finanza e controllo di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24 e 25);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- reati transnazionali (art. 10, L. 146/2006);
- Reati tributari (art. 25-quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un

sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire le attività di amministrazione, finanza e controllo.

Inoltre, è fatto espresso divieto di:

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;

b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;

c) effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a dipendenti di altre società private;

d) trasferire a qualsiasi titolo, se non per il tramite di banche o istituti di moneta elettronica o Poste Italiane S.p.A., 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 a quello previsto dalla vigente normativa;

e) emettere assegni bancari e postali per importi pari o superiori a quello previsto dalla vigente normativa che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;

f) girare per l'incasso assegni bancari e postali emessi all'ordine del traente a soggetti diversi da banche o Poste Italiane S.p.A.;

g) promettere o effettuate erogazioni in denaro a favore di rappresentati della Pubblica Amministrazione, per finalità diverse da quelle istituzionali e di servizio;

a) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio, del Collegio Sindacale o della società di revisione;

b) omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti dell'Autorità di Vigilanza, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalla predetta autorità;

c) esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;

d) indurre taluno in errore utilizzando artifici o raggiri ai fini di conseguire un ingiusto profitto in danno dello Stato, di altro ente pubblico o dell'Unione Europea. In particolare, si raccomanda il rispetto della legge e della corretta pratica commerciale a fronte di trattative, concessioni, licenze, ecc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;

e) assecondare la condotta induttiva di un pubblico ufficiale o di un incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità;

f) indicare nelle dichiarazioni fiscali elementi passivi fittizi;

g) porre in essere operazioni simulate;

h) richiedere, predisporre fatture od altra documentazione per operazioni inesistenti;

i) porre in essere documenti falsi per alterare i risultati fiscali e ridurre il carico delle imposte;

j) occultare e/o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione;

k) alienare beni per rendere infruttuosa la riscossione coattiva ai fini fiscali (es. eseguire pagamenti a beneficio di fornitori e terzi per non interrompere la continuità aziendale, sottraendo di conseguenza risorse al corretto adempimento dei tributi dovuti).

Protocolli specifici di prevenzione

a) Gestione della contabilità generale, con particolare riferimento alle attività di:

- rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (es. gestione e registrazione contabile della fatturazione attiva);

- verifica dati provenienti dai sistemi informativi alimentanti;

- raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato.

Per l'attività sensibile Gestione della contabilità generale, con particolare riferimento alle attività di rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (es. gestione e registrazione contabile della fatturazione attiva), verifica dati provenienti dai sistemi informativi alimentari, raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato, i protocolli prevedono che:

- le registrazioni contabili possono essere effettuate esclusivamente da soggetti abilitati nell'uso del sistema informatico adottato, in accordo ai livelli autorizzativi previsti dalla Società;
- ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto; pertanto, è compito del dipendente a ciò incaricato, fare in modo che la documentazione di supporto sia facilmente reperibile e ordinata secondo criteri logici;
- devono essere pianificate le attività necessarie alla chiusura dell'esercizio sociale e alla redazione del progetto di Bilancio secondo un calendario che deve essere comunicato a tutti i soggetti coinvolti nel processo;
- i Direttori/Responsabili di funzione che forniscono dati e informazioni relative al bilancio, hanno l'obbligo di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse che viene archiviata e conservata a cura della Funzione responsabile di tale attività sensibile;
- tutte le informazioni strumentali al processo valutativo o di stima delle voci di bilancio devono essere archiviate sotto la responsabilità delle Funzioni aziendali che producono/ricevono tali informazioni;
- le operazioni "fuori bilancio", in particolare le eventuali operazioni relative a derivati, devono essere riflesse a bilancio previa valutazione preliminare affidata ad un soggetto qualificato esterno all'organizzazione aziendale e nel rispetto di uno specifico iter autorizzativo tracciabile;
- nelle procedure di riferimento sono definite le soglie di rilevanza quantitativa al di sopra delle quali la Funzione competente deve provvedere ad effettuare *check* specifici e mirati sulle poste di bilancio

interessate;

- qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure correnti, deve essere previsto che la funzione preposta informi tempestivamente l'Organismo di Vigilanza;
- i documenti riguardanti la formazione delle decisioni che governano le operazioni delle attività a rischio sopra indicate, nonché quelli che danno attuazione alle decisioni devono essere archiviati e conservati a cura della funzione competente per l'operazione;
- ogni modifica ai dati contabili deve essere effettuata dalla sola Direzione/Funzione che li ha generati, garantendo la tracciabilità dell'operazione di modifica e previa formale autorizzazione del Direttore/Responsabile di Funzione;
- per ciascuna funzione deve essere individuato un responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al Collegio Sindacale previa verifica della loro completezza, inerenza e correttezza;
- le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal Collegio Sindacale, devono essere documentate e conservate a cura del responsabile di funzione, o da un suo delegato;
- tutti i documenti all'ordine del giorno delle riunioni dell'Assemblea o del Consiglio di Amministrazione relativi a operazioni sulle quali il Collegio Sindacale debba esprimere parere devono essere messi a disposizione di quest'ultimo con ragionevole anticipo rispetto alla data della riunione;
- deve essere sempre garantita la tracciabilità di fonti e informazioni nei rapporti con il Soci e il Collegio Sindacale;
- che tutte le fatture ricevute siano, a fronte di impegni di spesa, formalizzate attraverso un contratto o un ordine di acquisto;
- in mancanza di specifica documentazione di supporto dell'avvenuta ricezione merci o prestazione del servizio, la registrazione della fattura deve avvenire solo a fronte di adeguato memo redatto e firmato dalla funzione richiedente che specifichi le motivazioni della mancanza della documentazione stessa;
- sia verificata la corrispondenza tra il documento di trasporto (DDT) e la quantità di merce ricevuta o i servizi resi;
- sia verificata la corrispondenza tra l'OdA, l'entrata merce/servizi resi e la fattura;
- sia garantito un meccanismo di controllo della validità economica dell'operazione e della sua effettività oggettivamente e soggettivamente sostanziale;
- sia verificata la corrispondenza del totale delle fatture emesse (inclusa l'IVA effettivamente incassata);
- deve essere garantita l'adozione di strumenti specifici di controllo circa il regime IVA applicato alle fatture emesse dal cliente (ad es.: tramite presentazione di lettera d'intento), sulla base di indici di potenziali anomalia (quali, ad esempio, con riferimento ai clienti "esportatori abituali", l'evidenziazione di soggetti richiedenti costituitisi nei 12 mesi precedenti all'operazione intrattenuta o da intrattenere con la Società);
- sia assicurata la rilevazione di tutti i fatti amministrativi aziendali attivi che hanno riflesso economico e patrimoniale;
- sia garantita la tracciabilità del processo decisionale tramite documentazione e archiviazione (telematica e/o cartacea) di ogni attività del ciclo attivo; in particolare, ad ogni operazione di cessione

di beni/servizi deve corrispondere un ordine di acquisto inviato dal committente, un contratto, la documentazione attestante l'esecuzione della transazione (es. time-sheet, relazioni, report, etc.).

b) Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività:

- **autorizzazione e invio dei pagamenti;**
- **Inserimento / modifica delle coordinate bancarie del fornitore.**

Per l'attività sensibile Gestione dei flussi finanziari (ciclo attivo e passivo), tesoreria e provvista finanziaria, con particolare riferimento alle attività di autorizzazione e invio dei pagamenti e inserimento/modifica delle coordinate bancarie del fornitore, i protocolli prevedono che:

- deve essere sempre prevista la rilevazione e l'analisi di pagamenti/incassi ritenuti anomali per controparte, importo, tipologia, oggetto, frequenza o entità sospette;
- deve essere previsto un iter approvativo rafforzato per l'esecuzione di operazioni di incasso e pagamento che vedano coinvolti soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;
- devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone;
- le operazioni che comportano utilizzo o impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie devono avere sempre una causale espressa e essere documentate e registrate in conformità con i principi di professionalità e correttezza gestionale e contabile. Il processo operativo e decisionale deve essere tracciabile e verificabile nelle singole operazioni;
- deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza dei destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione; in particolare dovrà essere precisamente verificato che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- deve essere verificata la congruità delle provvigioni pagate ai collaboratori esterni (es. agenti) rispetto a quelle praticate nell'area geografica di riferimento;
- deve essere previsto il divieto di utilizzo del contante, ad eccezione dell'uso per importi non significativi della cassa interna, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie nonché il divieto di accettazione ed esecuzione di ordini di pagamento provenienti da soggetti non identificabili;
- per la gestione dei flussi in entrata e in uscita, devono essere utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione europea o enti creditizi/finanziari situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- in mancanza di specifica documentazione di supporto la registrazione della fattura deve avvenire solo a fronte di adeguato memo redatto e firmato dalla funzione richiedente che specifichi le motivazioni della mancanza della documentazione stessa;
- devono essere vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minime di spesa espressamente autorizzate dalla funzione amministrazione, ed in particolare per le operazioni di piccola cassa;
- deve essere predisposto un flusso informativo sistematico che garantisca il costante allineamento fra procure/poteri, deleghe operative e profili autorizzativi residenti nei sistemi informativi;

- deve essere effettuata attività di riconciliazione, sia dei conti intercompany, sia dei conti intrattenuti con istituti di credito;
- è prevista un'analisi circa eventuali profili di scostamento dei budget ed analisi di *trend*;
- sono previsti attori diversi operanti nelle seguenti fasi/attività del processo:
  a) richiesta della disposizione di pagamento per assolvere l'obbligazione;
  b) effettuazione del pagamento;
  c) controllo/riconciliazioni a consuntivo;
- deve essere assicurata l'individuazione chiara e tracciata del referente responsabile del fornitore (ruolo ricoperto, indirizzo mail, riferimenti aziendali, sede/ufficio);
- deve essere previsto un meccanismo di controllo della validità economica dell'operazione e della sua effettività oggettivamente e soggettivamente sostanziale;
- deve essere assicurata la tracciabilità del processo decisionale tramite documentazione e archiviazione (telematica e/o cartacea) di ogni attività del ciclo passivo; in particolare, ad ogni operazione di acquisto di beni e/o di servizi deve corrispondere una richiesta di acquisto debitamente autorizzata, un ordine di acquisto, un contratto, la documentazione attestante l'esistenza del fornitore, la relativa competenza, l'esecuzione della transazione (scheda informativa, identificazione ai fini IVA, bolla di consegna, documenti di traporto, time-sheet, relazioni, etc.);
- deve essere assicurata la rilevazione di tutti i fatti amministrativi aziendali passivi che hanno riflesso economico e patrimoniale.

c) Gestioni dei rapporti con gli istituti finanziari.

Per l'attività sensibile Gestione dei rapporti con gli istituti finanziari i protocolli prevedono che:

- per la gestione dei flussi in entrata e in uscita, devono essere utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione europea o enti creditizi/finanziari situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- è garantita l'adeguata suddivisione dei compiti e delle responsabilità ed un congruo sistema di autorizzazione delle operazioni ove a nessuno siano attribuiti poteri illimitati e i ruoli siano chiaramente definiti in coerenza al livello di responsabilità assegnata;
- le operazioni sono verificabili e documentabili;
- le modifiche, integrazioni o cancellazioni dei poteri di firma e delega devono derivare sempre da una apposita delibera del Consiglio di Amministrazione;
- deve essere effettuata la riconciliazione di tutti i saldi di conto corrente con le relative schede contabili, sulla base degli estratti conto bancari.

d) Gestioni dei crediti.

Per l'attività sensibile Gestione dei crediti i protocolli prevedono:

- la presenza di un nucleo centrale responsabile del monitoraggio e del coordinamento accentrato del processo di gestione dei crediti commerciali;
- la definizione delle strategie di gestione del credito in funzione della tipologia di controparte (Cliente/Rivenditore), della rilevanza del Cliente (fatturato) e del valore dello scaduto;
- un approccio progressivo nella gestione del credito scaduto al crescere dell'*ageing* della posizione;

- la definizione di modalità (ad es. sollecito verbale, sollecito scritto) attraverso le quali attuare la procedura di recupero del credito.

e) Rapporti con gli organi di controllo (es. Collegio Sindacale, Società di Revisione, ecc.) relativamente alle verifiche sulla gestione amministrativa/contabile, compresa la custodia e tenuta dei libri contabili e sociali.

Per l'attività sensibile Rapporti con gli organi di controllo (es. Collegio Sindacale, Società di Revisione, ecc.) relativamente alle verifiche sulla gestione amministrativa/contabile, compresa la custodia e tenuta dei libri contabili e sociali i protocolli prevedono che:

- deve essere identificato il personale preposto alla trasmissione della documentazione alla società di revisione;
- l'OdV garantisce la massima trasparenza e collaborazione al responsabile della Società di revisione, che ha la facoltà di contattarli per verificare congiuntamente situazioni che possano presentare aspetti di criticità in relazione alle ipotesi di reato considerate;
- tutti i documenti contabili relativi agli argomenti indicati nell'ordine del giorno delle riunioni del Consiglio di Amministrazione devono essere completi e messi a disposizione degli Amministratori con ragionevole anticipo rispetto alla data della riunione;
- l'accesso ai documenti già archiviati deve essere consentito solo alle persone autorizzate in base alle procedure operative aziendali, al Collegio Sindacale, alla Società di Revisione e all'Organismo di Vigilanza;
- la trasmissione delle informazioni deve essere consentita alle sole persone autorizzate e avvenire attraverso mezzi tecnici che garantiscano la sicurezza dei dati e la riservatezza delle informazioni;
- sono definite le responsabilità e le modalità operative di gestione dell'informazione e della documentazione d'impresa, compresi i documenti contabili, che sono redatti secondo quanto previsto dalla normativa vigente, ivi comprese le modalità e le tempistiche di conservazione e archiviazione, di modo da impedire successive modifiche e agevolare futuri controlli;

f) Rapporti Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo.

Per l'attività sensibile Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo i protocolli prevedono:

- siano definiti i criteri di determinazione e gestione dei prezzi di trasferimento, con indicazione del perimetro di applicazione degli stessi, ove sia necessario (es. ambito *Transfer Price*);
- sia definita chiaramente la funzione responsabile della definizione delle caratteristiche del contratto *intercompany*;
- siano definite delle attività di monitoraggio dei rapporti infragruppo;
- sia effettuata un'attività di riconciliazione dei conti *intercompany*;
- tutte le fatture ricevute devono essere, a fronte di impegni di spesa, formalizzate attraverso un contratto o un ordine di acquisto;
- sia verificata la corrispondenza tra il documento di trasporto (DDT) e la quantità di merce ricevuta o i servizi resi;
- sia verificata la corrispondenza tra l'OdA, l'entrata merce/servizi resi e la fattura.
- le movimentazioni di *cash pooling* sono tracciabili e monitorate tramite sistema di *remote banking* e sistema gestionale Gamma Enterprise;

- le movimentazioni di *cash pooling* sono verificate dall'addetto ufficio Pagamenti e Tesoreria: (i) con cadenza giornaliera tramite il sistema *remote banking*; (ii) con cadenza trimestrale tramite la riconciliazione dei saldi di inizio e fine trimestre tratti dal modulo di tesoreria con quelli risultanti in co.ge., interrogando lo specifico conto di contabilità generale acceso al rapporto di *cash pooling*;
- è definito il contratto che disciplinale modalità e i principi con i quali sono gestiti i rapporti tra la Società e le Società controllate, collegate e controllanti;
- sono descritte all'interno del contratto *intercompany* le attività svolte per conto della controparte;
- ciascuna operazione *intercompany* avviene sulla base di documentazione autorizzata da soggetti dotati di idonei poteri;
- per le fatture ricevute ed emesse dalla Società a fronte dell'acquisto o della vendita di beni e servizi infragruppo, la registrazione contabile avviene solo dopo che è verificata l'effettiva corrispondenza delle stesse dalla tramite il processo di Ciclo Passivo – con riferimento sia all'esistenza della transazione, sia all'importo della stessa come indicato in fattura – ai contratti, agli ordini di acquisto o alle conferme d'ordine in essere.
- è fatto espresso divieto di effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a dipendenti di altre società private;

g) Rimborsi spese, anticipi e spese di rappresentanza.

Per l'attività sensibile Rimborsi spese, anticipi e spese di rappresentanza i protocolli prevedono che:

- la gestione dei rimborsi spese deve avvenire in accordo con la normativa, anche fiscale, applicabile;
- i processi di autorizzazione e controllo delle trasferte devono essere sempre ispirati a criteri di economicità e di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e delle normative fiscali vigenti;
- nello svolgimento di attività di servizio devono essere sempre ricercate le soluzioni più convenienti, sia in termini di economicità che di efficienza operativa;
- il sostenimento di spese di rappresentanza deve soddisfare il concetto di "opportunità" della spesa, in linea pertanto con gli obiettivi aziendali;
- le spese per forme di accoglienza e di ospitalità devono attenersi ad un criterio di contenimento dei costi entro limiti di normalità;
- nei rapporti con interlocutori appartenenti alla Pubblica Amministrazione è fatto divieto di effettuare spese di rappresentanze (rimborso viaggi, soggiorni ecc.) ingiustificate;
- deve sempre essere indicato il nominativo del beneficiario di eventuali spese di rappresentanza;
- devono ritenersi assolutamente vietate tutte le spese in qualunque modo dirette ad acquisire vantaggi impropri;
- l'Ufficio Amministrazione è responsabile del controllo formale, di completezza, correttezza e inerenza dei giustificativi e di correttezza fiscale (per il rimborso spese);
- l'anticipo concesso al dipendente è oggetto di verifica conguaglio (a debito o credito) e riconciliazione dietro presentazione da parte del dipendente della spesa autorizzata dal relativo Responsabile e dei relativi giustificativi;
- tutte le spese di rappresentanza devono essere tali da non compromettere l'integrità o la reputazione di una delle parti e da non essere interpretate, da un osservatore imparziale, come finalizzate ad acquisire vantaggi o trattamenti di favore in modo improprio;

- venga assicurata la tracciabilità delle note spese e dei relativi giustificativi.

h) Gestione degli adempimenti fiscali

Per l'attività sensibile Gestione degli adempimenti fiscali si rende necessario assicurare:

- il rispetto dei protocolli di controllo in materia di registrazioni contabili previsti nella sezione a) che precede;
- il rispetto della strategia fiscale adottata a livello di gruppo e, in particolare, dei principi da applicare nella gestione della fiscalità e dei flussi informativi verso la controllante da parte delle società controllate;
- l'adozione di uno scadenziario fiscale che stabilisca anche la periodicità delle attività di monitoraggio circa il rispetto delle scadenze fiscali;
- l'adozione di meccanismi di controllo che assicurino che ad ogni voce di costo/ricavo sia riconducibile una fattura o qualsivoglia altra documentazione che attesti l'esistenza della transazione;
- che le variazioni in aumento e/o in diminuzione riportate nelle dichiarazioni dei redditi (IRES e IRAP) siano supportate da adeguata documentazione e da motivazioni conformi alla normativa fiscale applicabile;
- che i dati e le informazioni riportate nelle dichiarazioni IVA siano conformi e coerenti con i Registri IVA e con le liquidazioni effettuate;
- che le imposte versate (IRES, IRAP, IVA, ritenute) siano conformi e coerenti con i dati e le informazioni riportate nelle dichiarazioni fiscali;
- il rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette e indirette;
- l'adozione di meccanismi di revisione periodica della corretta esecuzione degli adempimenti fiscali;
- ove ci si avvalga di un consulente terzo nella predisposizione ed invio delle dichiarazioni fiscali, la sottoscrizione di apposito contratto nel quale inserire clausole standard circa l'accettazione incondizionata da parte del consulente dei principi di cui al D.lgs. 231/2001 e del Codice Etico della Società, nonché l'assunzione di responsabilità in capo al consulente circa la presentazione delle dichiarazioni fiscali nei termini di legge
- una periodica attività di formazione rivolta al personale aziendale coinvolto nella gestione di tale attività sensibile al fine di assicurare il corretto espletamento delle attività rilevanti, anche in relazione all'evoluzione normativa e delle prassi in materia fiscale (es. Circolari dell'Agenzia delle Entrate e altri informative tecniche).

i) Archiviazione della documentazione contabile e fiscale

Per l'attività sensibile Archiviazione della documentazione contabile e fiscale è necessario assicurare:

- la regolare tenuta e conservazione delle scritture contabili obbligatorie ai fini delle imposte sui redditi e dell'imposta sul valore aggiunto;
- l'effettuazione di verifiche periodiche sulle scritture contabili;
- il rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette e indirette, in materia di termini e condizioni di conservazione della documentazione contabile e fiscale;
- l'adozione di un trasparente, efficace ed efficiente sistema di archiviazione della documentazione contabile e fiscale;
- l'indicazione veritiera e corretta e relative comunicazioni del luogo di tenuta e conservazione delle scritture contabili;

- la corretta individuazione delle funzioni aziendali incaricate e legittimate alla tenuta (e movimentazione) dei registri;
- l'individuazione dei soggetti deputati e le modalità di segnalazione agli organi competenti in caso di eventi accidentali che possono deteriorare le scritture;
- un meccanismo di controllo e monitoraggio del trasferimento ad archivio remoto e/o distruzione di documentazione, ammissibili solo ove siano decorsi i termini di decadenza dell'accertamento fiscale.

Area di rischio: Gestione delle attività di amministrazione, finanza e controllo

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND *	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione della contabilità generale, con particolare riferimento alle attività di: - rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (es. gestione e registrazione contabile della fatturazione attiva); - verifica dati provenienti dai sistemi informativi alimentanti; - raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato.		✓													✓	SOC/CP - La Società inserisce in bilancio o in altri documenti contabili informazioni false al fine di ingannare soci e pubblico. RT – Nell'ambito delle attività di redazione e approvazione del bilancio, la Società determina artificiosamente delle voci di costo e di ricavo, anche avvalendosi di documenti e/o altri elementi giustificativi artefatti rispetto ai reali accadimenti aziendali.
Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività: - autorizzazione e invio dei pagamenti; - inserimento/modifica delle coordinate bancarie del fornitore.	✓	✓	✓				✓								✓	PA - La Società utilizza le disponibilità finanziarie al fine di condizionare indebitamente la Pubblica Amministrazione per ottenere indebiti vantaggi. SOC/CP - La Società utilizza le risorse finanziarie al fine di compiere atti di corruzione. RIC - La Società effettua pagamenti in contanti per riciclare denaro proveniente da attività illecite. CRI/TSN - La Società utilizza le disponibilità finanziarie come fondi per finanziare un'associazione criminosa al fine di ottenere in cambio indebiti vantaggi derivanti dall'operato della stessa. RT - Nei rapporti con fornitori esterni di beni e servizi, la Società determina in modo artificioso gli elementi passivi, avvalendosi di fatture passive emesse da fornitori esterni facenti riferimento a prestazioni non realmente eseguite (oggettivamente inesistenti), in tutto o in parte.
Gestione dei rapporti con gli istituti finanziari.		✓														SOC/CP – La Società corrompe un esponente di un istituto finanziario al fine di ottenere condizioni bancarie favorevoli per l'accensione di un finanziamento.
Gestione dei crediti.	✓	✓													✓	PA - La Società offre ad un pubblico ufficiale denaro o altra utilità per indurlo ad accelerare i tempi di pagamento di un credito. SOC/CP - La Società offre denaro o altra utilità al legale di una società controparte per indurlo ad accelerare i tempi di pagamento di un credito. RT - Nell'ambito della gestione delle posizioni creditizie, la Società emette documenti relativi ad operazioni inesistenti al fine di consentire al cliente l'evasione delle imposte sui redditi o dell'Iva, nell'interesse o a vantaggio della Società (ad es.: per favorire la vendita di prodotti e/o servizi offerti dalla Società stessa).
Rapporti con gli organi di controllo (es. Collegio Sindacale, Società di Revisione, ecc.) relativamente alle verifiche sulla gestione amministrativa/contabile, compresa la custodia e tenuta dei libri contabili e sociali.		✓														SOC/CP - La Società inserisce in bilancio o in altri documenti contabili informazioni false al fine di ingannare soci e pubblico.
Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo.		✓	✓				✓								✓	SOC/CP - La Società stipula contratti di servizi tra le diverse società del Gruppo, in tutto o in parte fittizi, al fine di creare le disponibilità finanziarie con le quali perpetrare atti di corruzione. RIC - La Società utilizza fatture *intercompany* per riciclare denaro proveniente da illeciti o contabilizza operazioni commerciali fittizie tra società appartenenti al medesimo gruppo al fine di ridurre il carico fiscale o procurare provviste necessarie per commettere reati di corruzione. CRI/TSN - La Società in accordo con due o più enti appartenenti al Gruppo pone in essere operazioni anche fittizie, finalizzate alla frode fiscale. RT - Nell'ambito dei rapporti infragruppo, la Società determina

															artificiosamente il prezzo dei servizi prestati, avvalendosi di fatture passive infragruppo, relative e prestazioni fittizie, in tutto o in parte.
Rimborsi spese, anticipi e spese di rappresentanza.	✔	✔												✔	PA - La Società riconosce rimborsi spese, in tutto o in parte fittizi, al fine di creare le disponibilità finanziarie per perpetrare reati di corruzione di pubblici ufficiali o di incaricati di pubblico servizio. SOC/CP - La Società riconosce rimborsi spese, in tutto o in parte fittizi, al fine di creare le disponibilità finanziarie per perpetrare reati di corruzione verso soggetti privati appartenenti ad un'altra società. RT - Nell'ambito della gestione dei rimborsi spese a personale dipendente e terzi soggetti, la Società si avvale di fatture o altri documenti giustificativi relativi a spese fittizie a fronte di trasferte non effettivamente avvenute.
Gestione degli adempimenti fiscali														✔	RT - Nell'ambito della gestione degli adempimenti fiscali, la Società indica in una delle dichiarazioni elementi passivi inesistenti o elementi attivi per un ammontare inferiore a quello effettivo.
Archiviazione della documentazione contabile e fiscale														✔	RT – La Società, al fine di evadere le imposte sui redditi o in materia di IVA, distrugge la propria documentazione contabile o i documenti di cui è obbligatoria la conservazione così da rendere impossibile la ricostruzione dei propri redditi o del proprio volume d'affari.

SEZIONE F – Gestione delle operazioni straordinarie

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione delle operazioni straordinarie, ed in particolare alle attività sensibili:

- Gestione delle operazioni straordinarie (es. M&A).
- Gestione delle operazioni sul capitale sociale (esempio emissione *bond*).

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione delle operazioni straordinarie di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- abusi di mercato (art. 25-sexies);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- reati transnazionali (art. 10, L. 146/2006);
- reati tributari (art. 25-quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire le operazioni straordinarie.

Protocolli specifici di prevenzione

a) Gestione delle operazioni straordinarie (es. M&A).

Per l'attività sensibile Gestione delle operazioni straordinarie (es. M&A), i protocolli prevedono che:

- siano preventivamente svolti sulla controparte anche straniera, ove possibile, dell'operazione idonei accertamenti strumentali a verificare l'identità, la sede, la natura giuridica, il certificato di iscrizione alla Camera di Commercio con l'attestazione (antimafia) che nulla osta ai fini dell'art. 10 della Legge 575/1965 – o equivalente nel caso di controparti estere, ove possibile - del soggetto cedente o del soggetto acquirente a qualsiasi titolo;

- siano preventivamente svolti accertamenti per verificare la sussistenza in capo alla controparte dell'operazione di condanne definitive o di procedimenti penali (es. carichi pendenti, precedenti penali) dai quali potrebbero derivare condanne ai sensi e agli effetti del Decreto;
- sia predisposta l'idonea documentazione a supporto dell'operazione proposta, nonché una relazione informativa preliminare che illustri i contenuti, l'interesse sottostante e le finalità strategiche dell'operazione;
- sia verificata preliminarmente la completezza, inerenza e correttezza della documentazione di supporto dell'operazione;
- tutte le operazioni straordinarie siano sottoposte e approvate dal Consiglio d'Amministrazione delle Società;
- la Società svolge attività di *due diligence* che consistono nella raccolta delle informazioni rilevanti dell'azienda in processo di acquisizione e nella loro verifica, al fine di esprimere un giudizio sul suo valore di mercato e sul suo possibile rendimento, nonché di valutare eventuali rischi fiscali connessi all'operazione (anche con il coinvolgimento di consulenti specializzati ove necessario);
- deve essere assicurata la segregazione di ruoli e responsabilità tra chi evidenzia l'opportunità di effettuare un'operazione societaria, chi la esegue e chi effettua il relativo controllo;
- la verifica della presenza di conflitto di interesse nella gestione dell'operazione societaria;
- deve essere garantito il monitoraggio dei poteri anche con riferimento alla verifica delle firme dei documenti inerenti le operazioni societarie;
- la documentazione redatta ed in genere ogni altra informazione formalizzata relativa all'operazione deve contenere solo elementi assolutamente veritieri ed essere coerente rispetto all'oggetto dell'operazione stessa.

b) Gestione delle operazioni sul capitale sociale (esempio emissione *bond*).

Per l'attività sensibile Gestione delle operazioni sul capitale sociale (esempio emissione *bond*) i protocolli prevedono che:

- la società di revisione e il Collegio Sindacale devono esprimere motivato parere sull'operazione ove previsto dalla normativa;
- tutte le operazioni straordinarie siano sottoposte e approvate dal Consiglio d'Amministrazione delle Società.
- è fatto espresso divieto di:
  - restituire conferimenti ai soci o liberarli 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;
  - effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
  - procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale.

Infine, per quanto concerne l'attività di gestione delle operazioni sul capitale sociale, si applicano tutti quei protocolli previsti all'interno della Sezione M, per l'attività di gestione delle informazioni privilegiate e comunicazioni al mercato.

Area di rischio: Gestione delle operazioni straordinarie

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione delle operazioni straordinarie (es. M&A).		✔	✔				✔								✔	SOC/CP - Gli amministratori della Società compiono operazioni di fusione o scissione in violazione di disposizioni di legge alterando l'integrità del capitale sociale a discapito dei creditori; gli amministratori della Società corrompono gli amministratori della società target di un progetto di acquisizione. RIC - La Società stipula accordi al fine di trasferire denaro proveniente da attività illecite (interne/esterne) per poi reimpiegarlo in attività lecite (auto-riciclaggio). CRI/TSN - La Società intrattiene rapporti (es. partnership, joint venture) e/o effettua operazioni di acquisizione o dismissione di società o rami d'azienda con soggetti legati ad associazioni per delinquere, al fine di conseguire un vantaggio per la Società. RT – La Società determina in modo artificioso il prezzo di un'operazione straordinaria, anche mediante documentazione artefatta, eventualmente prodotta con la collaborazione di terzi, a supporto dei connessi processi di *due diligence* e decisionali.
Gestione delle operazioni sul capitale sociale (esempio emissione bond).										✔						MA - Porre in essere operazioni simulate o altri artifizi al fine di alterare il prezzo di strumenti finanziari non quotati

SEZIONE G – Gestione dei sistemi informativi e della sicurezza informatica

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione dei sistemi informativi e della sicurezza informatica, ed in particolare alle attività sensibili:

- Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, *account* e profili);
- Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni;
- Gestione della progettazione e della installazione dei *software* applicativi aziendali interni;
- Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT;
- Gestione, tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso;
- Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione dei sistemi informativi e della sicurezza informatica di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- delitti informatici e trattamento illecito di dati (art. 24-bis);
- delitti in materia di violazione del diritto d'autore (art. 25-novies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

La Società risulta, inoltre, dotata di un sistema di gestione della sicurezza delle informazioni conforme ai seguenti standard:

- ISO/IEC 27001:2013: "Erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura Cloud (IaaS)"; e
- ISO/IEC 27018:2014 per la protezione dei dati personali nei servizi Public Cloud.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire i sistemi informativi e garantire la sicurezza informatica.

Inoltre, è fatto espresso divieto:

a) accedere in maniera non autorizzata ai sistemi informativi utilizzati da soggetti privati o dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare informazioni a vantaggio dell'azienda o di terzi, o comunque al fine di procurare un indebito vantaggio all'azienda od a terzi;

b) per tutti i dipendenti: (i) introdursi abusivamente o permanere contro la volontà espressa o tacita

dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza; (ii) procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo;

c) distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda;

d) distruggere, danneggiare, rendere in tutto o in parte inservibile sistemi informatici o telematici altrui o della Società ovvero ostacolarne gravemente il funzionamento;

e) intercettare fraudolentemente, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;

f) rivelare, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle comunicazioni fraudolentemente intercettate relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;

g) procurarsi, riprodurre, diffondere comunicare o consegnare codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o, comunque, fornire indicazioni o istruzioni idonee al predetto scopo;

h) formare falsamente (sia sotto il profilo materiale sia per quanto attiene al contenuto) documenti societari aventi rilevanza esterna;

i) procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o comunque mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti;

j) utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio *virus*, *worm*, *troian*, *spyware*, *dialer*, keylogger, *rootkit*) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Protocolli specifici di prevenzione

a) Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni.

Per l'attività sensibile Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, *account* e profili), i protocolli prevedono che:

- la Società deve definire, aggiornare e approvare formalmente le policy aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e all'accesso remoto da parte di terzi soggetti;
- la Società deve gestire il processo di nomina di amministratore/i di sistema e amministratore/i di database con atto formale, definizione di compiti e attribuzioni ed espressa assunzione della relativa responsabilità nel rispetto di quanto previsto dal Provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008 e successive modifiche o integrazioni;
- la Società deve far rispettare il sistema di gestione delle utenze, con particolare riferimento alla definizione di nuove utenze e della loro cancellazione;
- qualora l'attività sia svolta in service da un soggetto il terzo il rapporto deve essere regolato da apposito contratto di servizio;
- deve essere effettuata una distinzione tra tipologie di utenti per l'installazione di software specifici e tutti gli utenti risultano amministratori della propria macchina;
- deve essere effettuata verifica periodica dei profili di accesso, di concessione di utenze e della modifica dei profili.

- l'identificazione dell'utente per l'accesso alle informazioni deve avvenire attraverso un identificativo univoco preventivamente assegnatogli;
- devono essere definiti dei criteri e le modalità (ad es. lunghezza minima, regole di complessità, scadenza) per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili;
- la corretta gestione delle password deve essere definita da linee guida, comunicate a tutti gli utenti, per la selezione e l'utilizzo della *password*;
- tutte le utenze abilitate, sia quelle associate ai dipendenti che ai Clienti o ai fornitori, sono sottoposte a revisione circa la sussistenza delle esigenze che hanno portato alla loro attivazione. La revisione delle utenze avviene periodicamente con frequenza almeno semestrale;
- è definita una tabella contenente i software di base che devono essere installati sul pc dell'utente all'atto dell'assunzione.

b) Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni.

Per l'attività sensibile Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni, i protocolli prevedono che:

- la Società deve definire, aggiornare e approvare formalmente le policy aziendali, le procedure in materia di sicurezza informatica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai profili di autorizzazione dei singoli utenti;
- qualora l'attività sia svolta in service da un soggetto il terzo il rapporto deve essere regolato da apposito contratto di servizio, che preveda l diritto di audit da parte di TS sul rispetto dei *service level agreement* concordati (SLA);
- devono essere definiti dei criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- è predisposta una matrice autorizzativa – applicazioni/profili/richiedente – allineata con i ruoli organizzativi in essere e coerente con i principi di segregazione dei ruoli.

c) Gestione della progettazione e della installazione dei *software* applicativi aziendali interni.

Per l'attività sensibile Gestione della progettazione e della installazione dei *software* applicativi aziendali interni, i protocolli prevedono che:

- la Società deve definire, aggiornare e approvare formalmente le *policies* aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e all'accesso remoto da parte di terzi soggetti;
- la società deve definire una chiara politica di controllo degli accessi negli ambienti di sviluppo e deve costantemente verificarne l'applicazione;
- qualora l'attività di supporto è svolta da personale esterno, la Direzione IT deve mettere a disposizione all'utente uno specifico account;
- tutte le attività svolte dagli operatori con ruolo di Amministratori di Sistema devono essere appropriatamente tracciate;

d) Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT

Per l'attività sensibile Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT, i protocolli prevedono che:

- la Società deve regolamentare in modo chiaro e formalizzato l'accesso fisico ai locali in cui risiedono le infrastrutture IT (attribuzione di facoltà di accesso, misure di sicurezza e di vigilanza e assunzione della relativa responsabilità);
- deve essere assicurata la tracciabilità delle persone che hanno avuto accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT;
- deve essere definito il processo di *reporting* delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza e le contromisure da attivare;
- la documentazione riguardante le attività deve essere conservata, ad opera del Responsabile della Funzione coinvolta, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- devono essere definite le misure di sicurezza adottate, le modalità di vigilanza, la relativa frequenza e le responsabilità nell'ambito della gestione degli accessi fisici;
- devono essere definite, implementate e comunicate ai soggetti coinvolti le procedure che stabiliscano la necessità di credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, codici di accesso, badge, e la tracciabilità degli stessi;
- l'accesso alla sala CED di Pesaro è riservato alle persone esterne della società con un contratto di manutenzione degli apparati (es. condizionatori, rete dati e fonia, ecc.) e ai dipendenti della società individuati dalla Direzione IT e dalla Direzione HR;
- le chiavi ed i tag degli accessi ai locali sono assegnati tramite lettera nominativa;
- la società di manutenzione effettua il monitoraggio remoto della temperatura, dei dispositivi antincendio e dell'impianto elettrico, degli UPS presenti nella sala CED.

e) Gestione, tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso.

Per l'attività sensibile Gestione, tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso, i protocolli prevedono che:

- la Società deve adottare una procedura che gestisca l'inventario degli *asset* a supporto delle attività di gestione, che permetta di mantenere la visibilità dello stato delle risorse e ne faciliti la manutenzione, l'implementazione e la gestione e manutenzione di reti;
- la Società deve promuovere controlli finalizzati a garantire la gestione e la manutenzione *hardware* e *software* (ivi compresi l'inventario e i divieti o limitazioni di utilizzo) e deve attivare procedure di controllo di installazione di software potenzialmente pericolosi sui sistemi operativi;
- per i software acquistati o comunque in uso da parte della Società, il database comprende anche i seguenti dati:

  a) data di acquisto della licenza;

  b) data di scadenza della licenza;

  c) tipo di utilizzo autorizzato dal contratto di licenza;

- sono svolte verifiche periodiche sui software installati al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;

f) Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici.

Per l'attività sensibile Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici, i protocolli prevedono che:

- la Società deve definire, aggiornare e approvare formalmente le policy aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento al piano di *back up*, *disaster recovery* e alla gestione della posta elettronica;
- la Società deve promuovere l'utilizzo di sistemi crittografici nella creazione, emissione, archiviazione, conservazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;
- la Società deve promuovere momenti di allineamento fra esigenze di business e sistema informativo, ad esempio all'interno di un comitato di indirizzo periodico in cui siano esplicitate le esigenze strategiche e di allineamento con le relative priorità siano monitorate le attività di adeguamento, e siano assicurate le risorse necessarie;
- deve essere eseguito un *Vulnerability Assessment* per la ricerca sistematica delle vulnerabilità di un sistema/applicazione o di una rete, al fine di fornire una valutazione del grado di adeguatezza delle misure di protezione poste in essere;
- deve essere eseguito un *Penetration Test* per la verifica sul campo in modo sistematico, se e come le vulnerabilità riscontrate siano sfruttabili da parte di un attaccante esperto;
- devono essere sottoposti all'attenzione dell'Amministratore di Sistema tutti i dispositivi, *files* o programmi di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa;
- deve essere prestata particolare attenzione ai supporti rimovibili contenenti Dati Sensibili, per evitare che il loro contenuto possa essere recuperato anche dopo la loro cancellazione.

Area di rischio: Gestione dei sistemi informativi e della sicurezza informatica

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	
Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, account e profili).				✔											IT – La Società si introduce abusivamente in un sistema telematico per ottenere informazioni che portano un interesse o vantaggio per la Società.
Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni.				✔											IT – La Società accede e danneggia il sistema informatico/telematico di terze parti per creare un disservizio ad un competitor al fine di procurare un interesse o vantaggio alla Società stessa.
Gestione della progettazione e della installazione dei software applicativi aziendali interni.				✔											IT – La Società diffonde un programma capace di infettare il sistema informativo di un Ente Pubblico al fine di posticipare i termini fissati per la presentazione delle offerte necessari per la partecipazione a gare d'appalto.
Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT.				✔											IT – La Società si introduce in aree sottoposte a misure di sicurezza per diffondere, installare apparecchiature, dispositivi o programmi informatici volti a distruggere, manomettere, o cancellare informazioni al fine di ottenerne un vantaggio.
Gestione e tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso.				✔							✔				IT - Soggetti installano apparecchiature HW o SW interne o esterne alla società al fine di carpire informazioni che possono essere di interesse o vantaggio per la società. DA – I dipendenti della Società duplicano abusivamente programmi coperti da licenza al fine di trarne vantaggi economici (consistenti nel risparmio rispetto all'acquisto dei programmi).
Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici.				✔											IT – La Società si introduce in aree sottoposte a sequestro da parte delle Autorità per distruggere, manomettere, o cancellare informazioni al fine di ottenerne un vantaggio.

SEZIONE H – Approvvigionamento di beni e servizi

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio approvvigionamento di beni e servizi, ed in particolare alle attività sensibili:

- Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività:

- gestione dell'albo fornitori;

- selezione del fornitore e valutazione dei requisiti qualificanti;

- stipula di accordi quadro di fornitura;

- emissione degli ordini;

- Gestione degli acquisti di consulenze ed assegnazione incarichi professionali a terzi.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio approvvigionamento di beni e servizi di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- delitti contro la personalità individuale (art. 25-quinquies);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- reati transnazionali (art. 10, L. 146/2006);
- reati tributari (art. 25-quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire l'approvvigionamento di beni e servizi.

Inoltre, è fatto espresso divieto di:

a) effettuare prestazioni in favore dei consulenti, dei *Partner* e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;

b) utilizzare informazioni su clienti, fornitori, operatori acquisite illecitamente al fine di ottenere benefici di qualunque utilità nelle relazioni commerciali;

c) effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a dipendenti di altre società private;

Protocolli specifici di prevenzione

a) Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività:

- **Gestione dell'albo fornitori;**
- **Selezione del fornitore e valutazione dei requisiti qualificanti;**
- **Stipula di accordi quadro di fornitura;**
- **Emissione degli ordini.**

Per l'attività sensibile Gestione degli acquisti di beni e servizi, con particolare riferimento alle attività di gestione dell'albo fornitori, selezione del fornitore e valutazione dei requisiti qualificanti, stipula di accordi quadro di fornitura ed emissione degli ordini, i protocolli prevedono che:

- devono esistere norme aziendali relative all'approvvigionamento di particolari tipologie di beni e servizi (consulenze, prestazioni professionali) ovvero relative ad approvvigionamenti con particolari modalità attuative (es. con riferimento al fornitore unico, o in caso di urgenza);
- le norme aziendali devono essere ispirate, in ciascuna fase del processo di approvvigionamento, a criteri di trasparenza (precisa individuazione dei soggetti responsabili, valutazione delle richieste di approvvigionamento, verifica che le richieste arrivino da soggetti autorizzati, determinazione dei criteri che saranno utilizzati nelle varie fasi del processo e tracciabilità delle valutazioni sulle offerte tecniche ed economiche) e di tracciabilità delle operazioni effettuate;
- la scelta della modalità di approvvigionamento da adottare (es. pubblicazione del bando, fornitore unico, utilizzo di *vendor list* qualificate) deve essere formalizzata e autorizzata a un adeguato livello gerarchico;
- deve essere garantito il rispetto dei compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo e dalle procedure vigenti nel processo di acquisto di beni e servizi;
- deve essere garantito il rispetto dei principi di correttezza e trasparenza e garanzia dell'integrità e della reputazione delle parti nei rapporti intrattenuti con i fornitori;
- deve essere garantita la tracciabilità e trasparenza nella definizione dell'esigenza di acquisto e nell'individuazione del fornitore;
- deve essere acquisito l'impegno formale da parte dell'affidatario dei lavori ad uniformarsi alle prescrizioni del Codice Etico ed alle linee di condotta del Modello e al Codice di Condotta Anti Corruzione al fine di sanzionare eventuali comportamenti contrari ai principi etici aziendali;
- deve essere ottenuta una dichiarazione di assenza di rapporti preesistenti tra il fornitore e la Pubblica Amministrazione ostativi all'affidamento della fornitura;
- deve essere identificata una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard;
- devono essere determinati adeguati criteri di selezione, selezione, stipulazione ed esecuzione di accordi/*joint venture* con altre imprese per la realizzazione di investimenti;
- siano previsti attori diversi operanti nelle seguenti fasi/attività del processo:

  a) richiesta della fornitura;

b) effettuazione dell'acquisto;

c) certificazione dell'esecuzione dei servizi/consegna dei beni (rilascio benestare);

d) effettuazione del pagamento;

- siano individuate le scelte in merito al mantenimento della controparte all'interno dell'Albo fornitori o alla relativa cancellazione dalle medesime liste non possano essere determinate da un unico soggetto e siano sempre motivate;
- sia verificato, con riferimento agli acquisti *intercompany*, che la fornitura di beni o di servizi sia avvenuta a condizioni di mercato;
- sia verificata sulla sussistenza dei requisiti normativi di regolarità della controparte tramite la consegna della documentazione prevista dalla legge (ad es. documento unico di regolarità contributiva – DURC ed iscrizione alla camera di commercio);
- nei contratti di fornitura, deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- tutte le fatture ricevute siano, a fronte di impegni di spesa, formalizzate attraverso un contratto o un ordine di acquisto;
- sia presente un'adeguata e documentabile giustificazione di tutti i compensi e le somme corrisposte ai Fornitori nel rapporto contrattuale in essere con il Fornitore;
- sia presente un'adeguata attività selettiva dei Fornitori e determinate le condizioni d'acquisto di beni e servizi sulla base di valutazioni motivate ed imparziali, fondate sulla qualità, sul prezzo e sulle garanzie fornite;
- siano individuati degli indicatori di anomalia per l'identificazione di eventuali transazioni "a rischio" o "sospette" con le controparti;
- siano individuati dei criteri in base ai quali la controparte può essere cancellata dall'Albo Fornitori della Società.

b) Gestione degli acquisti di consulenze ed assegnazione incarichi professionali a terzi.

Per l'attività sensibile Gestione degli acquisti di consulenze ed assegnazione incarichi professionali a terzi, i protocolli prevedono che:

- deve essere prevista l'esistenza di attori diversi operanti nelle differenti fasi del processo di gestione delle consulenze (ad es. non vi deve essere coincidenza di identità tra chi richiede la consulenza, chi la autorizza e chi esegue il pagamento della prestazione);
- deve essere effettuata un'adeguata attività selettiva fra i diversi operatori di settore;
- devono essere utilizzati idonei dispositivi contrattuali adeguatamente formalizzati;
- devono esistere adeguati livelli autorizzativi (in coerenza con il sistema di procure aziendali) per la stipulazione dei contratti;
- devono essere presenti i livelli di approvazione per la formulazione delle richieste di consulenza e per la certificazione/validazione del servizio reso;
- devono esistere i requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e di meccanismi di valutazione complessiva del servizio reso;
- nell'impiego di consulenti esterni, nell'ambito della gestione dei rapporti con la PA, devono essere previsti dei meccanismi di verifica preventiva dell'assenza di conflitti di interesse con le stesse amministrazioni pubbliche (per esempio mediante auto-certificazione del consulente esterno);

- nei contratti di fornitura, patti fra soci o *partner* commerciali, deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- devono esistere documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e archiviati;
- deve essere acquisito l'impegno formale da parte dei consulenti esterni ad uniformarsi alle prescrizioni del Codice Etico ed alle linee di condotta del Modello al fine di sanzionare eventuali comportamenti contrari ai principi etici aziendali;
- al termine dell'incarico, in caso di mancanza di documentazione attestante l'avvenuta esecuzione della prestazione, sia richiesto al Consulente di dettagliare per iscritto le prestazioni effettuate;
- il rapporto tra la Società e il consulente in area commerciale deve sempre risultare da incarico scritto non generico definendo in particolare i criteri di attribuzione delle provvigioni spettanti agli stessi;
- il consulente si deve impegnare formalmente ad astenersi dall'effettuare pagamenti, regali ovvero offerte o promesse di pagamento, mediante risorse proprie o messe a disposizione dalla Società, a pubblici ufficiali, enti pubblici, partiti politici, a persona fisica o giuridica che possa avere influenza sull'acquisizione del contratto col cliente;
- tutte le fatture ricevute siano a fronte di impegni di spesa formalizzati attraverso un contratto o un ordine di acquisto;
- sia presente un'adeguata e documentabile giustificazione di tutti i compensi e le somme corrisposte ai Fornitori nel rapporto contrattuale in essere con il Fornitore;
- sia presente un'adeguata attività selettiva dei Fornitori e determinate delle condizioni d'acquisto di beni e servizi sulla base di valutazioni motivate ed imparziali, fondate sulla qualità, sul prezzo e sulle garanzie fornite;
- siano individuati degli indicatori di anomalia per l'identificazione di eventuali transazioni "a rischio" o "sospette" con le controparti;
- sia predisposto ed aggiornato periodicamente l'elenco delle controparti.

Area di rischio: Approvvigionamento di beni e servizi

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività: - gestione dell'albo fornitori; - selezione del fornitore e valutazione dei requisiti qualificanti; - stipula di accordi quadro di fornitura; - emissione degli ordini.	✔	✔	✔				✔					✔			✔	PA - La Società affida consulenze fittizie a soggetti graditi o suggeriti al fine di aggiudicarsi commesse pubbliche. SOC/CP – La Società emette ordini di merci fittizi a soggetti graditi o suggeriti al fine di aggiudicarsi commesse private. RIC - La Società acquista beni sottocosto poiché provenienti da attività illecite o investe i proventi derivanti da attività corruttive nell'acquisto di beni (auto-riciclaggio). CRI/TSN - La Società stipula un contratto con un fornitore collegato alla criminalità organizzata al fine di ottenere indebiti vantaggi. PI - Il fornitore utilizza personale senza rispettare quanto previsto dal CCNL. RT - mediante una determinazione artificiosa degli elementi passivi, attraverso il fittizio accordo con un procacciatore, omettendo attività di verifica sull'esistenza e sull'operatività reale dello stesso.
Gestione degli acquisti di consulenze ed assegnazione incarichi professionali a terzi.	✔	✔	✔				✔								✔	PA - La Società assegna un contratto ad una società di consulenza collegata ad un esponente della PA al fine di ottenere indebiti vantaggi. SOC/CP – La Società affida consulenze fittizie a soggetti graditi o suggeriti al fine di aggiudicarsi commesse pubbliche o private. RIC – La Società crea fondi neri, tramite fatture di consulenza fittizie, allo scopo di utilizzarli a scopo corruttivo. CRI/TSN - La Società crea fondi neri, tramite fatture di consulenza fittizie, da utilizzare come finanziamenti ad associazioni criminali al fine di ottenere vantaggi dall'operato delle stesse. RT - Nell'ambito della gestione dei rapporti con consulenti e prestatori d'opera esterni, attraverso una determinazione non veritiera (in eccesso) di voci di costo.

SEZIONE I – Progettazione e commercializzazione di software applicativi per elaboratori

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio progettazione e commercializzazione di *software* applicativi per elaboratori, ed in particolare alle attività sensibili:

- Gestione delle attività connesse alla progettazione e allo sviluppo di *software* applicativi con particolare riguardo ai clienti e distributori;
- Gestione dei rapporti con clienti diretti con particolare riferimento alle seguenti attività:
  - gestione dell'anagrafica clienti;
  - partecipazione a gare private;
  - definizione della scontistica da applicare;
  - formalizzazione dell'offerta;
  - evasione dell'ordine;
  - richieste di documentazione da parte dei clienti al fine dell'emissioni di finanziamenti al cliente.
- Partecipazione a bandi per assegnazione di pubbliche forniture, compresa la gestione dei rapporti con la PA in caso di vittoria del bando di gara;
- Gestione del *customer support* e delle attività post-vendita;
- Gestione delle attività di *delivery*;
- Gestione delle vendite dei servizi standard anche tramite *e-commerce*.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio progettazione e commercializzazione di *software* applicativi per elaboratori di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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);
- delitti informatici e trattamento illecito di dati (art. 24-bis);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis);
- reati societari (art. 25-ter);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- delitti in materia di violazione del diritto d'autore (art. 25-novies);
- reati transnazionali (art. 10, L. 146/2006);
- reati tributari (art. 25-quinquiesdecies).

Infine, si precisa che la fattispecie di reato frode nell'esercizio del commercio è stata considerata come non applicabile in quanto si riferisce esclusivamente a beni mobili. Tuttavia, la Società ha implementato comunque protocolli di controlli tali da mitigare il rischio di commissione di reati contro l'industria e il commercio.

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di progettare e commercializzare *software* applicativi per elaboratori.

Inoltre, è fatto espresso divieto di:

a) impiegare per finalità aziendali beni tutelati da diritti acquisiti in elusione dei relativi obblighi o comunque con modalità difformi da quelle previste dal titolare;

b) impiegare beni aziendali al fine di porre in essere condotte che violino la tutela dei diritti d'autore, quale che sia il vantaggio perseguito.

c) esibire documenti e dati incompleti e/o comunicare dati falsi e alterati;

d) sottrarre o omettere l'esibizione di documenti veri;

e) omettere informazioni dovute;

f) alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;

g) indurre taluno in errore utilizzando artifici o raggiri ai fini di conseguire un ingiusto profitto in danno dello Stato, di altro ente pubblico o dell'Unione Europea. In particolare, si raccomanda il rispetto della legge e della corretta pratica commerciale a fronte di trattative, concessioni, licenze, ecc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;

h) assecondare la condotta induttiva di un pubblico ufficiale o di un incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità;

i) sviluppare un *software* contenente un *malware* o installare *backdoor*, utile ad procurarsi informazioni dei clienti al fine di ottenere un vantaggio.

Protocolli specifici di prevenzione

a) Gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi con particolare riguardo ai clienti e distributori.

Per l'attività sensibile Gestione delle attività connesse alla progettazione e allo sviluppo di *software* applicativi con particolare riguardo ai clienti e distributori, i protocolli prevedono che:

- siano adottate Linee Guida per lo sviluppo sicuro del software in conformità alle best practice di settore (es. OWASP);
- deve essere garantita la tracciabilità delle attività connesse allo sviluppo di nuovi prodotti e servizi;

- nella fase di studio di fattibilità del progetto devono essere valutati possibili conflitti con titoli di proprietà industriale altrui;
- deve essere assicurata la possibilità di ricostruire tutte le fasi che hanno portato allo sviluppo di un nuovo *software*;
- i processi autorizzativi devono essere sempre accuratamente documentati e verificabili a posteriori;
- devono essere formulati inviti generali al rispetto delle norme in materia di proprietà intellettuale;
- devono essere elaborate clausole riferite all'osservanza anche da parte dei terzi contraenti delle norme in materia di proprietà intellettuale;
- siano controllati i mezzi di comunicazione interni ed esterni alla società (es. *sito web*, radio ufficiale, stampa, e altri canali ancora), in grado di diffondere opere protette;
- nel caso particolare in cui gli illeciti contro la proprietà intellettuale si realizzino con l'impiego di sistemi informatici aziendali, possono rivelarsi utili anche le misure auspicabili per la prevenzione dei reati informatici richiamati dagli artt. 24, 24-bis e 25-quinquies del decreto 231, quali ad esempio lo sviluppo, la gestione e il monitoraggio delle infrastrutture informatiche o la presenza del cd. supervisore informatico;
- siano monitorati fenomeni quali: (i) *Undelicensing*: violazioni delle condizioni di licenza di un *software*; (ii) *Hard disk loading*: vendita e relativo acquisto per l'azienda di computer sui quali sono installati; (iii) utilizzazione non autorizzata di banche dati;
- nella fase di sviluppo di nuovi prodotti, siano condotte indagini in merito all'eventuale utilizzo di marchi o segni distintivi che potrebbero risultare similari a quelli di proprietà altrui. In particolare, all'interno dei contratti siglati con sviluppatori, partner esterni, fornitori e/o di acquisizione (M&A) sia sempre prevista una clausola che preveda il diritto di autore e tutela della società;

b) Gestione dei rapporti con clienti diretti con particolare riferimento alle seguenti attività:

- **gestione dell'anagrafica clienti;**
- **partecipazione a gare private;**
- **definizione della scontistica da applicare;**
- **formalizzazione dell'offerta;**
- **evasione dell'ordine;**
- **richieste di documentazione da parte dei clienti al fine dell'emissioni di finanziamenti al cliente.**

Per l'attività sensibile Gestione dei rapporti con clienti diretti, con particolare riferimento alle attività di gestione dell'anagrafica clienti, partecipazione a gare private, definizione della scontistica da applicare, formalizzazione dell'offerta, evasione dell'ordine, emissioni di finanziamenti al cliente, i protocolli prevedono che:

- i processi autorizzativi devono essere sempre accuratamente documentati e verificabili a posteriori;
- i rapporti con i clienti devono essere verificabili attraverso documentazione contrattuale completa e idonea a definire chiaramente ogni obbligo/diritto di entrambe le parti;
- le controparti commerciali devono essere preventivamente verificate, attraverso le informazioni disponibili, al fine di accertare la relativa rispettabilità e affidabilità prima di avviare rapporti d'affari, assicurando la tracciabilità degli accertamenti svolti;
- le operazioni commerciali devono essere supportate da adeguata documentazione, secondo le modalità specifiche previste dalle procedure aziendali applicabili al processo in oggetto, e devono avvenire entro le linee guida stabilite dalla Società;

- deve essere identificata una funzione responsabile della valutazione delle offerte nei contratti standard;
- deve essere effettuato un confronto tra il prezzo dell'offerta rispetto a quello di mercato e un eventuale passaggio autorizzativo in caso di scostamenti significativi;
- deve essere assicurata una gestione controllata dell'emissione dell'ordine di vendita e delle successive eventuali modifiche;
- sia implementato un sistema di reporting verso il Responsabile della Funzione coinvolta contente informazioni in merito ai clienti o potenziali clienti incontrati, esito degli incontri, principali problematiche emerse, ecc.;
- la scontistica ai clienti diretti è elaborata mediante il sistema CRM all'interno del quale è stata predisposta una matrice di sconti, applicati ed approvati secondo i livelli di autorizzazione definiti;
- esclusivamente per quanto concerne la Direzione International, l'elenco dei prezzi viene definito congiuntamente dalla Funzione International Business e dai clienti del paese in questione;
- i clienti internazionali di grande dimensione sono preventivamente verificati, attraverso appositi controlli che garantiscono a TeamSystem S.p.A. di accertare la relativa rispettabilità ed affidabilità prima di avviare rapporti d'affari;
- sia adottata una specifica procedura o altro strumento normativo aziendale per la gestione delle richieste di accesso ai finanziamenti pubblici da parte dei clienti;
- è fatto espresso divieto di:

a) utilizzare informazioni su clienti, fornitori, operatori acquisite illecitamente al fine di ottenere benefici di qualunque utilità nelle relazioni commerciali;

b) omettere informazioni su clienti, fornitori, consulenti giudicate sensibili ai fini del compimento dei reati di cui alla presente parte speciale.

c) Partecipazione a bandi per assegnazione di pubbliche forniture, compresa la gestione dei rapporti con la PA in caso di vittoria del bando di gara.

Per l'attività sensibile partecipazione a bandi per assegnazione di pubbliche forniture, compresa la gestione dei rapporti con la PA in caso di vittoria del bando di gara, i protocolli prevedono che:

- le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono gestiti esclusivamente dai soggetti aziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- tutti i contratti aventi come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;
- tutta la documentazione deve essere verificata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;

- non vi è identità soggettiva tra il soggetto che procede alle negoziazioni nei limiti assegnati ed il soggetto che approva definitivamente l'accordo, apponendovi la propria sottoscrizione;
- tutti gli incontri sono formalizzati attraverso e-mail o lettera di sintesi, all'interno della quale vengono sintetizzate le richieste del cliente. Ciascun incontro viene registrato all'interno del CRM, dove vengono riportati i nominativi dei partecipanti ed allegato il "memo" dell'incontro;
- siano predisposte attività di monitoraggio degli SLA di progetto.

d) Gestione del *customer support* e delle attività post vendita.

Per l'attività sensibile gestione del *customer support* e delle attività post vendita, i protocolli prevedono che:

- sia vietato divulgare qualsiasi dato, informazione o materiale di proprietà altrui, acquisito durante gli accessi ai sistemi di terze parti, e deve essere prevista la cancellazione coerentemente con quanto previsto dalla normativa sulla protezione dei dati;
- venga effettuato un monitoraggio costante del possesso dei requisiti specificati nel contratto con la Pubblica Amministrazione e a quanto dichiarato alla stessa in merito ai servizi di *customer support* e di attività post-vendita**;**
- sia assicurata la tracciabilità delle azioni svolte dagli utenti;
- i momenti preposti al controllo delle attività di assistenza, sono le riunioni di revisione che, a loro volta, sono cadenzate con passo mensile;
- gli operatori di assistenza monitorano il corretto svolgimento delle attività mantenendo sorvegliata la coda di *ticket* aperti.
- gli utenti preposti sono dotati di log nominativi che consentono la tracciabilità delle loro attività;
- l'accesso a sistemi informativi o telematici di terze parti avviene esclusivamente previa autorizzazione delle stesse.

e) Gestione delle attività di *delivery*.

Per l'attività sensibile gestione delle attività di *delivery* i protocolli prevedono che:

- sia previsto il divieto di divulgare qualsiasi dato, informazione o materiale di proprietà altrui, acquisito durante gli accessi ai sistemi di terze parti, e si preveda la cancellazione coerentemente con quanto previsto dalla normativa sulla protezione dei dati;
- sia effettuato un costante monitoraggio del possesso dei requisiti specificati nel contratto con la Pubblica Amministrazione e a quanto dichiarato alla stessa in merito ai servizi di *delivery*.
- la tracciabilità e il monitoraggio degli accessi ai sistemi informativi di terze parti;
- l'accesso a sistemi informativio telematici di terze parti avvenga esclusivamente previa autorizzazione delle stesse.

f) Gestione delle vendite dei servizi standard anche tramite *e-commerce*.

Per l'attività sensibile gestione delle vendite dei servizi standard anche tramite *e-commerce* i protocolli prevedono che:

- sia predisposta una scheda informativa per ciascun prodotto contenente le caratteristiche da riportare sul sito;

- siano previsti adeguati livelli autorizzativi (in coerenza con il sistema di procure aziendali) per la definizione dei listini e del corretto aggiornamento dei dati sul sito web;
- la gestione dei siti web sia in conformità alle prescrizioni di legge in vigore;
- sia prevista una verifica circa la corrispondenza tra le caratteristiche dei prodotti posti in vendita (e-commerce) e quanto riportato sul materiale informativo o comunque su qualsiasi materiale diffuso al pubblico.

Area di rischio: Progettazione e commercializzazione di *software* applicativi per elaboratori

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi con particolare riguardo ai clienti e distributori.				✓							✓		✓			IT - La Società sviluppa un software contenente un malware utile ad procurarsi informazioni dei clienti al fine di ottenere un vantaggio. DA - La Società nell'ambito della attività di progettazione potrebbe astrattamente sviluppare TSW sfruttando indebitamente proprietà intellettuale altrui. FA - La Società commercializza software il cui marchio risulta contraffatto.
Gestione dei rapporti con clienti diretti con particolare riferimento alle seguenti attività: - gestione dell'anagrafica clienti; - partecipazione a gare private; - definizione della scontistica da applicare; - formalizzazione dell'offerta; - evasione dell'ordine - emissioni di finanziamenti al cliente.		✓	✓				✓								✓	SOC/CP - La Società condiziona indebitamente i rappresentanti di una società privata al fine di stipulare contratti di vendita di prodotti. RIC- La Società non avendo accertato l'identità della controparte, stipula contratti di vendita incassando consapevolmente somme di denaro di provenienza delittuosa. CRI/TSN - La Società stipula accordi di partnership con clienti legati ad associazioni criminali, nell'esecuzione del contratto stesso, commettono reati finalizzati ad apportare vantaggi al business della Società. RT - Nell'ambito della cessione di servizi alla clientela, sono emessi documenti relativi ad operazioni inesistenti al fine di consentire al cliente l'evasione delle imposte sui redditi o dell'Iva, nell'interesse o a vantaggio della Società (ad es.: per favorire la vendita di prodotti e/o servizi offerti dalla Società stessa).
Partecipazione a bandi per assegnazione di pubbliche forniture, compresa la gestione dei rapporti con la PA in caso di vittoria del bando di gara.	✓															PA - La Società, al fine di garantirsi la partecipazione alle procedure di gara, ovvero l'aggiudicazione, in assenza o anche in presenza dei requisiti minimi previsti dal bando, potrebbe offrire o promettere indebite utilità a Pubblici Ufficiali o Incaricati di Pubblico Servizio.
Gestione del customer support e delle attività post-vendita.	✓			✓											✓	PA - Il cliente appartenente alla PA sottoscrive un contratto inclusivo di determinate prestazioni che non vengono erogate. IT - L'incaricato della società accede abusivamente ai sistemi informatici durante le azioni di customer support presso il cliente. RT - Nell'ambito della gestione dei servizi post vendita, sono emessi documenti relativi ad operazioni inesistenti al fine di consentire al cliente l'evasione delle imposte sui redditi o dell'Iva, nell'interesse o a vantaggio della Società (ad es.: per favorire la vendita di prodotti e/o servizi offerti dalla Società stessa).
Gestione delle attività di delivery.	✓	✓		✓												PA - Il cliente appartenente alla PA sottoscrive un contratto inclusivo di determinate prestazioni che non vengono erogate. SOC/CP - La Società fattura servizi non prestati o prestati e non conformi a quanto stabilito contrattualmente. IT - L'incaricato della Società accede abusivamente ai sistemi informatici durante le azioni di delivery presso il cliente.
Gestione delle vendite dei servizi standard anche tramite e-commerce.		✓														SOC/CP - La Società vende prodotti a prezzo inferiore a quello di mercato al fine di corrompere controparti private.

SEZIONE J – Gestione delle partnership

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio *gestione delle partnership*, ed in particolare alle attività sensibili:

- Gestione dei rapporti con società private con le quali si intende stipulare accordi di partnership, con particolare riferimento alle seguenti attività:

- individuazione delle opportunità di partnership commerciali/tecnologiche;

- definizione degli accordi con i Partner.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione delle *partnership* di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- reati transnazionali (art. 10, L. 146/2006);
- reati tributari (art. 25-quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire le *partnership*.

Protocolli specifici di prevenzione

a) Gestione dei rapporti con società private con le quali si intende stipulare accordi di partnership, con particolare riferimento alle seguenti attività:

- individuazione delle opportunità di *partnership* commerciali/tecnologiche;

- definizione degli accordi con i *Partner*.

Per l'attività sensibile Gestione dei rapporti con società private con le quali si intende stipulare accordi di *partnership*, con particolare riferimento alle attività di individuazione delle opportunità di *partnership* commerciali/tecnologiche e di definizione degli accordi con i *Partner*, i protocolli prevedono che:

- le Funzioni che richiedono la selezione e l'assunzione di agenti devono formalizzare la richiesta attraverso la compilazione di modulistica specifica e nell'ambito di un budget annuale;
- nella fase di "individuazione e scelta dell'agente professionista", devono essere verificati i requisiti di professionalità, integrità, onestà ed affidabilità, attraverso:
    - compilazione e sottoscrizione di un Questionario di Auto-Certificazione;
- le informazioni raccolte in fase iniziale di impostazione del rapporto dovranno essere periodicamente aggiornate;
- nella fase di "Contrattualizzazione", i contratti redatti in collaborazione con funzione legale devono:
    - essere definiti avendo a riferimento i prezzi medi di mercato applicati al servizio oggetto di acquisto;
    - prevedere una specifica clausola che vincoli agenti all'osservanza dei principi etico-comportamentali adottati dalla Società. La mancata osservanza di tale clausola, da sottoscrivere espressamente, dovrà essere indicata come possibile causa di scioglimento del rapporto contrattuale;
    - escludere l'utilizzo di clausole ambigue che possano indurre a comportamenti non conformi ai principi etico-comportamentali quali, ad esempio, il riferimento all'adozione di generici provvedimenti atti a superare le criticità nelle procedure autorizzative;
- nella fase di "Controllo e valutazione della prestazione", deve essere previsto:
    - lo svolgimento di specifica attività formativa, nel periodo iniziale del rapporto (inserimento), per gli agenti che svolgono correntemente attività in contatto con la P.A.;
    - l'effettuazione di periodica attività valutativa circa la qualità del servizio reso e della rispondenza dei soggetti ai requisiti di selezione;
    - l'istituzione di una "*Black List*" infragruppo per la gestione delle informazioni relative a situazioni anomale rilevate e nominativi di agenti cessati per motivazioni ex decreto 231/2001;
- non devono essere corrisposte agli agenti provvigioni in misura non congrua rispetto alla natura e al valore della transazione conclusa, o non conformi alle condizioni commerciali o alle prassi esistenti sul mercato;
- i criteri di attribuzione degli incentivi e delle provvigioni spettanti agli agenti devono essere definiti in modo chiaro e trasparente e non essere basati solo sul parametro del maggior venduto, ma anche, a titolo esemplificativo e non esaustivo, sulla fidelizzazione dei clienti, sull'assenza di reclami rispetto all'operato, sul numero di clienti in portafoglio, ecc.
- la scelta del partner o la stipula di convenzioni deve avvenire nel rispetto di criteri predeterminati ed alla luce di indici di rischio ed anomalia preventivamente identificati e costantemente aggiornati dalle funzioni competenti;
- il rapporto sia disciplinato da contratto scritto, nel quale sia chiaramente prestabilito il valore della transazione o i criteri per determinarlo;
- nella selezione delle terze parti devono sempre essere espletati, qualora applicabili, gli adempimenti richiesti dalla normativa antimafia;
- devono essere preventivamente svolti accertamenti idonei a verificare l'identità, la sede e la natura

giuridica della controparte dell'operazione e siano svolti, ove compatibile con la normativa sulla protezione dei dati personali, verifiche finalizzate a prevenire il rischio di infiltrazioni criminali;

- i contratti che regolano i rapporti con la terza parte devono prevedere apposite clausole che indicano chiare responsabilità in merito al mancato rispetto degli eventuali obblighi contrattuali derivanti dall'accettazione dei principi fondamentali del Codice Etico, del Modello e del Codice di Condotta Anti Corruzione;
- siano svolte verifiche su eventuali comportamenti non conformi al Codice Etico e del Codice di Anti Corruzione della Società partner;
- siano effettuate verifiche in merito a possibili conflitti di interesse con la Pubblica Amministrazione;
- siano definiti adeguati livelli autorizzativi (in coerenza con il sistema di procure aziendali) per la stipulazione dei contratti, listini, campagne, prestazioni ecc.;
- sia garantita la tracciabilità della documentazione attraverso i sistemi gestionali di cui la Società si è dotata;
- i contratti con partner internazionali sono formalmente approvati dall'A.D. o da un soggetto dotato di idonei poteri, e le clausole contrattuali, vengono stipulate in collaborazione con l'Ufficio Legale e Affari Societari;
- i partner sono preventivamente verificati, attraverso l'analisi delle visure che garantiscono di ottenere informazioni utili e valutarne la solidità economica prima di avviare rapporti d'affari;
- sono sottoscritti contratti formali con *partner* tecnologici che mettono a disposizione soluzioni dedicate per lo sviluppo di *software* della TeamSystem S.p.A..I contratti prevedono delle clausole specifiche ed aggiuntive rispetto ai contratti standard di fornitura (es. SLA d'ingaggio);
- divieto di effettuare prestazioni in favore dei consulenti, dei *Partner* e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere.

Area di rischio: Gestione delle partnership

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Gestione dei rapporti con società private con le quali si intende stipulare accordi di partnership, con particolare riferimento alle seguenti attività: - individuazione delle opportunità di partnership commerciali/tecnologiche; - definizione degli accordi con i partner.	✔	✔	✔				✔								✔	PA – La Società stipula accordi di partnership con società composte da soggetti legati alla Pubblica Amministrazione al fine di ottenere indebiti vantaggi. SOC/CP - La Società condiziona indebitamente i rappresentanti di una società privata al fine di stipulare contratti di partnership maggiormente favorevoli. RIC - La Società non avendo accertato l'identità della controparte, stipula contratti di partnership incassando consapevolmente somme di denaro di provenienza delittuosa. CRI/TSN - La Società stipula accordi di partnership con agenti, partner commerciali legati ad associazioni criminali che, nell'esecuzione del contratto stesso, commettono reati finalizzati ad apportare vantaggi al business della Società. RT - Mediante una determinazione artificiosa degli elementi passivi, attraverso il fittizio accordo con un partner commerciale, omettendo attività di verifica sull'esistenza e sull'operatività reale dello stesso.

SEZIONE K – Gestione della Salute e Sicurezza sul Lavoro

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione della Salute e Sicurezza sul Lavoro, ed in particolare alle attività sensibili:

- Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali;
- Definizione delle risorse, dei ruoli, delle responsabilità e autorità nell'organizzazione;
- Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL;
- Gestione delle emergenze;
- Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.);
- Sorveglianza sanitaria;
- Definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori;
- Comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze;
- Gestione di incidenti non conformità e azioni correttive;
- Approvvigionamento e gestione degli appalti; acquisizione di documentazioni / certificazioni obbligatorie di legge.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione della Salute e Sicurezza sul Lavoro di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- omicidio colposo o lesioni colpose gravio gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire la Salute e la Sicurezza sul Lavoro.

Protocolli specifici di prevenzione

a) Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali.

Per l'attività sensibile Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali, i protocolli prevedono che:

- la conformità alle vigenti norme in materia (leggi, norme tecniche e regolamenti, ecc.) deve essere

assicurata attraverso l'adozione di specifiche registrazioni allo scopo di porre sotto controllo;

- sono identificate le leggi e le normative applicabili alle attività e ai prodotti della Società;
- è stabilito un controllo periodico della conformità alla normativa applicabile;
- sono individuati i soggetti responsabili dell'identificazione e valutazione dell'applicabilità della normativa vigente e sono identificate le fonti di approfondimento normativo consultabili;
- la Società si avvale delle funzioni di competenza per l'individuazione, divulgazione e monitoraggio degli aspetti legali, inclusi gli standard tecnico-strutturali.

b) Definizione delle risorse, dei ruoli, delle responsabilità e autorità nell'organizzazione.

Per l'attività sensibile definizione delle risorse, dei ruoli, delle responsabilità e autorità nell'organizzazione, i protocolli prevedono che:

- devono essere definite procedure, ruoli e responsabilità in merito alle fasi dell'attività di predisposizione e attuazione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori;
- devono essere definiti, in coerenza con le disposizioni di legge vigenti in materia, i meccanismi relativi a:

a) valutazione e controllo periodico dei requisiti di idoneità e professionalità del responsabile del servizio di prevenzione e protezione (c.d. "RSPP") e degli addetti al servizio di prevenzione e protezione (c.d. "ASPP");

b) definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;

c) processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza delle modalità e della tempistica in caso di avvicendamento nel ruolo;

- deve essere garantita la presenza e l'aggiornamento dell'Organigramma della Sicurezza di Sede/Società (es. RSPP, RLS, Medico Competente, Addetti antincendio e primo soccorso, Preposti), monitorando tempestivamente ogni cambiamento intercorso e/o di progetti di cambiamento tecnologico, impiantistico, organizzativo e procedurale;
- la Società si avvale delle funzioni di competenza per l'individuazione, divulgazione e monitoraggio degli aspetti legati agli standard tecnico-strutturali;
- è prevista, anche attraverso un sistema di deleghe, l'attribuzione di specifiche responsabilità, in data certa, attraverso la forma scritta definendo, in maniera esaustiva, caratteristiche e limiti dell'incarico e, se del caso, individuando il potere di spesa;
- sono formalizzate le relative responsabilità di gestione in maniera univoca, anche mediante specifici atti di nomina e il corretto conferimento di poteri necessari allo svolgimento del ruolo, inclusi quelli di spesa;
- sono correttamente nominati i soggetti previsti dalla normativa in materia di igiene e sicurezza dei luoghi di lavoro (ivi inclusi, nel caso di presenza di cantieri, i soggetti previsti dal titolo IV del D.Lgs. 81/2008) e sono loro conferiti adeguati poteri necessari allo svolgimento del ruolo agli stessi assegnato;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale è congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti situazioni di rischio;
- non vi è identità soggettiva fra coloro che assumono o attuano le decisioni e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo;
- i soggetti che rivestono un ruolo datoriale ai sensi del D.lgs. 81/08 sono formalmente designati dalla Società con la conseguente attribuzione di deleghe e procure in materia di gestione del personale,

nonché di tutela della salute dei lavoratori, ai fini di un'opportuna gestione delle tematiche di Salute e Sicurezza nei luoghi di lavoro; l'organigramma per la sicurezza è pubblicato nell'intranet aziendale, e indica compiti, poteri e responsabilità di tutti i soggetti investiti di incarichi nell'ambito dell'apparato aziendale di prevenzione dal rischio infortuni/malattie professionali, e la Società ne cura l'aggiornamento.

c) Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL.

Per l'attività sensibile identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL, i protocolli prevedono che:

- devono essere definiti i meccanismi di predisposizione dei Documenti di Valutazione dei Rischi ("DVR", "DUVRI") per la Salute e la Sicurezza sul Lavoro;
- deve essere predisposto un modello di monitoraggio sistemico e continuo dei dati/indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il sistema di prevenzione e protezione;
- deve essere prevista la consultazione preventiva dei rappresentanti dei lavoratori in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
- siano individuate le consulenze e le professionalità esterne necessarie e da coinvolgere nella valutazione dei rischi e nell'adeguamento documentale, tecnico, impiantistico;
- sia definito, aggiornato e divulgato, attraverso il supporto del RSPP, il Documento di Valutazione dei Rischi (DVR);
- sia effettuata la valutazione dei rischi, elaborando il D.V.R. e ogni altro documento necessario al mantenimento o miglioramento degli standard di salute e sicurezza;
- l'individuazione e la rilevazione dei rischi è competenza del datore di lavoro, che si avvale del supporto di altri soggetti quali il Responsabile del Servizio di Prevenzione e Protezione ed il medico competente previa consultazione del rappresentante dei lavoratori per la sicurezza;
- tutti i dati e le informazioni che servono alla valutazione dei rischi e conseguentemente all'individuazione delle misure di tutela (ad es. documentazione tecnica, misure strumentali, esiti di sondaggi interni, ecc.) devono essere chiari, completi e rappresentare in modo veritiero lo stato della Società;
- i dati e le informazioni sono raccolti ed elaborati tempestivamente, sotto la supervisione del datore di lavoro, anche attraverso soggetti da questo individuati in possesso di idonei requisiti, certificabili nei casi previsti, di competenza tecnica e, se del caso, strumentale;
- a richiesta, insieme ai dati ed alle informazioni, devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni;
- la Società procede all'identificazione e valutazione di tutti i rischi per la salute e sicurezza dei lavoratori che risultino significativi e di responsabilità della Società; i criteri, costituenti integrazione di tale identificazione, contemplano, tra gli altri, i seguenti aspetti:

  a) attività di routine e non routine;

  b) attività di tutte le persone che hanno accesso al posto di lavoro (compresi esterni);

  c) comportamento umano;

  d) pericoli provenienti dall'esterno;

  e) pericoli legati alle operazioni o creati nell'ambiente circostante;

  f) infrastrutture, attrezzature e materiali presenti presso il luogo di lavoro;

  g) modifiche apportate ai processi e/o al sistema di gestione, tra cui le modifiche temporanee, e il

loro impatto sulle operazioni, processi ed attività;

h) eventuali obblighi giuridici applicabili in materia di valutazione dei rischi e di attuazione delle necessarie misure di controllo;

- è disponibile, in adempimento al Testo Unico Sicurezza, per ciascuna unità locale, un Documento di Valutazione dei Rischi che individua i rischi operativi ed i possibili danni che si possono verificare nell'ambito delle varie aree di attività; il Documento di Valutazione dei Rischi è predisposto dalla Società;
- la Società individua le misure di prevenzione e di protezione adeguate per il controllo dei rischi ed elabora il programma di miglioramento mediante, tra l'altro:

  a) l'individuazione delle fonti potenziali di pericolo presenti in tutte le fasi lavorative;

  b) l'individuazione dei soggetti esposti;

  c) l'individuazione dei danni effettivamente verificatisi in passato, sulla base dell'esame delle statistiche degli infortuni e delle malattie professionali;

  d) la valutazione dei rischi, considerando adeguatezza e affidabilità delle misure di tutela, cui segue l'individuazione delle misure di eliminazione o riduzione dei rischi, con programmazione delle azioni di prevenzione e protezione;

- in relazione ai Dispositivi di Protezione Individuale, è necessario che la Società:

  a) identifichi le attività per le quali prevedere l'impiego di DPI e l'eventuale coinvolgimento dell'identificazione del MC e dell'RLS;

  b) definisca i criteri di scelta dei DPI, che devono assicurare l'adeguatezza dei DPI stessi alle tipologie di rischio individuate in fase di valutazione e la loro conformità alle norme tecniche vigenti (ad es. marcatura CE);

  c) definisca le modalità di consegna ed eventualmente di conservazione/manutenzione dei DPI;

  d) definisca un eventuale scadenzario per garantire il mantenimento dei requisiti di protezione e la definizione di specifiche azioni in caso di riscontro di non conformità a seguito delle verifiche svolte presso i magazzini.

d) Gestione delle emergenze.

Per l'attività sensibile gestione delle emergenze, i protocolli prevedono che:

- devono essere definiti, in coerenza con le disposizioni di legge vigenti in materia, i meccanismi relativi a:

  a) definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;

- il Piano Antincendio e d'Emergenza della Sede deve essere definito, aggiornato e divulgato, attraverso il supporto del RSPP;
- la gestione delle emergenze viene attuata attraverso specifici piani che prevedono:

  a) l'identificazione delle situazioni che possono causare una potenziale emergenza;

  b) definizione delle modalità per rispondere alle condizioni di emergenza e prevenire o mitigare le relative conseguenze negative in tema di salute e sicurezza;

  c) modalità e responsabilità di gestione delle prove di emergenza, con particolare riguardo alla tipologia di emergenza (es. incendio, evacuazione, ecc.);

  d) pianificazione ed esecuzione delle prove di emergenza per la verifica dell'efficacia dei piani di gestione delle emergenze, finalizzata ad assicurare la piena conoscenza da parte del personale delle corrette misure comportamentali e l'adozione di idonei strumenti di

registrazione atti a dare evidenza degli esiti di dette prove e delle attività di verifica e di manutenzione dei presidi predisposti;

e) sono individuati, attraverso detti piani, i percorsi di esodo e le modalità di attuazione, da parte del personale, delle misure di segnalazione e di gestione delle emergenze;

f) sono disponibili e mantenuti in efficienza idonei sistemi per la lotta agli incendi scelti per tipologia e numero in ragione della specifica valutazione del rischio di incendio ovvero delle indicazioni fornite dall'autorità competente; sono altresì presenti e mantenuti in efficienza idonei presidi sanitari;

g) è assicurata all'interno degli spazi operativi un'adeguata organizzazione delle attività produttive al fine di consentire la corretta esecuzione delle procedure di emergenza;

- ove applicabile, la Società provvede a ottenere il Certificato di Prevenzione Incendi (CPI) ai sensi del D.P.R 151/2011.

e) Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.).

Per l'attività sensibile definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.), i protocolli prevedono che:

- devono essere individuati i requisiti e le competenze specifiche per la conduzione delle attività di audit sul modello di Salute e Sicurezza dei lavoratori nonché le modalità e le tempistiche delle verifiche sullo stato di attuazione delle misure adottate;
- deve essere garantita l'idoneità degli edifici, la corretta manutenzione dei mezzi e attrezzature di lavoro, l'adempimento degli obblighi di legge;
- devono essere definite, aggiornate e divulgate, attraverso il supporto del RSPP, le istruzioni operative per la sicurezza delle postazioni di lavoro e/o delle mansioni lavorative;
- deve essere tenuta aggiornata la documentazione di propria competenza all'evolversi dei processi tecnici ed organizzativi della Sede/Società;
- deve essere assicurato l'aggiornamento della documentazione di sede/società e il calendario/scadenziario delle attività di miglioramento e implementazione;
- devono essere garantiti i controlli periodici previsti per legge su impianti, macchinari, attrezzature;
- la Società provvede a effettuare periodicamente le opportune verifiche e controlli di manutenzione presso i vari siti interessati (es. verifica impianti messa a terra, impianti antincendio);
- vengono effettuati sopralluoghi presso le diverse sedi, nei quali vengono notificate eventuali non conformità e programmati gli opportuni interventi risolutivi;
- sono definite le modalità di registrazione delle manutenzioni effettuate e le relative responsabilità;
- sono definite le modalità di segnalazione delle anomalie, individuati i mezzi più idonei per comunicare tali modalità, individuate le funzioni tenute ad attivare il relativo processo di manutenzione (manutenzioni non programmate);
- gli eventuali interventi specialistici sono condotti da soggetti in possesso dei requisiti di legge che devono produrre le necessarie documentazioni.

f) Sorveglianza sanitaria.

Per l'attività sensibile sorveglianza sanitaria i protocolli prevedono che:

- devono essere definiti, in coerenza con le disposizioni di legge vigenti in materia, i meccanismi relativi a:

  a) processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza delle modalità e della tempistica in caso di avvicendamento nel ruolo;

- deve essere garantita la formazione dei lavoratori della Società e il presidio sanitario previsto per legge;
- deve essere mantenuto aggiornato l'elenco del personale di Sede/Società da sottoporre o sottoposto a sorveglianza sanitaria, presidiando le scadenze, i cambi mansioni, le nuove assunzioni, il rispetto delle prescrizioni impartite dal medico competente;
- deve essere conservato in archivio il protocollo sanitario, la relazione annuale sullo stato di salute dei lavoratori, il verbale di sopralluogo del medico, fotocopia dei giudizi di idoneità;
- deve essere inviato al HSE *Manager* e al medico coordinatore l'elenco complessivo e aggiornato dei lavoratori al fine di consentire l'aggiornamento dello stato di attuazione della sorveglianza sanitaria da parte dei vari medici competenti nominati sul territorio;
- il medico competente deve effettuare almeno un sopralluogo annuale – e all'occorrenza ogni qual volta richiesto - agli ambienti di lavoro rilasciando relativo verbale scritto;
- deve essere assicurata l'attuazione della sorveglianza sanitaria;
- sono definite le modalità di verifica dei requisiti per quanto riguarda gli aspetti sanitari, se riscontrati in sede di valutazione del rischio, da effettuare preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore.

g) Definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori.

Per l'attività sensibile definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori, i protocolli prevedono che:

- sono previste attività di informazione e formazione di tutto il personale circa le corrette modalità di espletamento dei propri incarichi, nonché nei casi previsti dalla normativa;
- devono essere organizzati i corsi di formazione e addestramento necessari in funzione del programma formativo approvato dal Datore di Lavoro;
- devono essere segnalati eventuali carenze formative, informative e relative all'addestramento del personale in funzione dei rischi a cui è esposto e delle mansioni assegnate;
- la Società si avvale delle funzioni di competenza per l'individuazione, divulgazione e monitoraggio dei requisiti di competenza, abilità e consapevolezza necessari per lo svolgimento delle attività aziendali;
- le attuali modalità operative prevedono che la funzione HR si occupi di comunicare nuove assunzioni e cambio mansioni, per l'individuazione dei lavoratori da sottoporre alle attività formative;
- la Società provvede a monitorare le esigenze formative attraverso uno scadenziario con le schede relative a ciascun lavoratore;
- gli attestati e certificazioni di formazione del personale sono archiviati.

h) Comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze.

Per l'attività sensibile comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze, i protocolli prevedono che:

- devono essere previste riunioni periodiche con la dirigenza, con i lavoratori e i loro rappresentanti;
- deve essere garantito l'accesso delle informazioni al Rappresentante Dei Lavoratori per la sicurezza (RLS);
- deve essere coordinato il processo di coinvolgimento degli altri attori previsti dalla vigente normativa al fine di tenerli costantemente informati sugli obblighi di legge e sulle modalità di adeguamento agli stessi;
- deve essere convocata una riunione periodica almeno annuale - o all'occorrenza con maggiore frequenza - per discutere del Documento di Valutazione dei Rischi (DVR) e delle misure preventive e protettive individuate;
- la Società ha identificato dei Rappresentanti dei Lavoratori per la Sicurezza, che vengono consultati relativamente alla Valutazione dei Rischi;
- la Società svolge periodicamente la riunione periodica ai sensi dell'art. 35 del D.lgs. 81/2008;
- sono disciplinate specifiche modalità che regolamentano il coinvolgimento e la consultazione dei lavoratori, in particolare:

  a) la comunicazione interna tra i vari livelli e funzioni dell'organizzazione;

  b) la comunicazione con i fornitori ed altri visitatori presenti sul luogo di lavoro;

  c) il ricevimento e risposta alle comunicazioni dalle parti esterne interessate;

  d) la partecipazione dei lavoratori, anche a mezzo delle proprie rappresentanze, attraverso:

  e) il loro coinvolgimento nell'identificazione dei pericoli, valutazione dei rischi e definizione delle misure di tutela;

  f) il loro coinvolgimento nelle indagini relative ad un incidente;

  g) la loro consultazione quando vi siano cambiamenti che possano avere significatività in materia di salute e sicurezza.

i) Gestione di incidenti non conformità e azioni correttive.

Per l'attività sensibile gestione di incidenti non conformità e azioni correttive, i protocolli prevedono che:

- deve essere fornito il supporto tecnico e normativo alle sedi/società nella programmazione e nella risoluzione delle tematiche aperte, e nel mantenimento di standard di rispetto normativo;
- deve essere garantito l'accesso delle informazioni al Rappresentante dei Lavoratori per la sicurezza (RLS);
- devono essere attuate le azioni correttive e preventive di miglioramento individuate nelle riunioni periodiche della sicurezza e approvate dal DATORE DI LAVORO, presidiandone lo stato di avanzamento e valutandone gli effetti migliorativi; segnalare tempestivamente eventuali criticità nella messa in atto delle misure di cui sopra;
- devono essere raccolte e valutate le segnalazioni dei Preposti;
- la Società adotta ancora il registro infortuni per la registrazione e gestione degli incidenti sul lavoro (o in itinere);
- vengono effettuati sopralluoghi presso le diverse sedi, nei quali vengono notificate eventuali non conformità e programmati gli opportuni interventi risolutivi;
- sono definiti i ruoli, le responsabilità e le modalità di rilevazione, tracciabilità/registrazione e investigazione interna degli infortuni, incidenti occorsi e "*near miss*";
- sono definite le modalità di comunicazione da parte dei responsabili operativi al Datore di Lavoro e al responsabile del servizio di prevenzione e protezione sugli infortuni/incidenti occorsi;

- sono definiti i ruoli, le responsabilità e le modalità di monitoraggio degli infortuni occorsi (tenendo conto di eventuali controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro) al fine di identificare le aree a maggior rischio infortuni.

j) Approvvigionamento e gestione degli appalti; acquisizione di documentazioni / certificazioni obbligatorie di legge.

Per l'attività sensibile approvvigionamento e gestione degli appalti; acquisizione di documentazioni / certificazioni obbligatorie di legge, i protocolli prevedono che:

- devono essere predisposti un *budget*, piani annuali e pluriennali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza;
- devono essere definiti i meccanismi di predisposizione dei Documenti di Valutazione dei Rischi ("DVR", "DUVRI") per la Salute e la Sicurezza sul Lavoro;
- devono essere previsti meccanismi di controllo che garantiscano l'inclusione nei contratti di appalto, subappalto e somministrazione, dei costi relativi alla sicurezza del lavoro;
- deve essere garantito lo scambio informativo dei rischi con le Ditte Esterne incaricate di prestazioni di servizio, e presidiare l'andamento dei lavori relativamente ai rischi d'interferenza;
- sono incluse le clausole e le verifiche richieste in materia di salute e sicurezza per le attività di approvvigionamento e gestione degli appalti;
- devono essere definite le modalità di valutazione dei requisiti di salute e sicurezza degli stessi tenendo conto anche delle considerazioni dei lavoratori attraverso le loro rappresentanze da svolgere preliminarmente alle attività di acquisto di attrezzature, macchinari ed impianti;
- le attrezzature, i macchinari e gli impianti devono garantire la conformità a quanto previsto dalla normativa vigente (ad es. marcatura CE, possesso di dichiarazione di conformità rilasciata dall'installatore, ecc.);
- deve essere previsto che, se del caso, in ragione dei disposti legislativi applicabili, la messa in esercizio di attrezzature, macchinari e impianti sarà subordinata a procedure di esame iniziale o di omologazione;
- sono previste opportune attività di formazione e/o addestramento preliminarmente all'utilizzo di nuove attrezzature, macchinari o impianti da parte dei lavoratori incaricati;
- le attività di acquisto sono svolte con lo scopo di:
  a) definire i criteri e le modalità per la selezione, valutazione e qualifica dei fornitori, in particolare avendo riguardo a eventuali criticità in materia di SSL;
  b) definire le modalità e responsabilità della verifica;
- sono definite le modalità per la verifica della conformità dei beni e macchinari da acquistare alle normative vigenti (ad es. marcatura CE), nonché i criteri e le modalità per la valutazione dei requisiti di accettabilità;
- sono previste, qualora applicabili, le modalità di esecuzione dei controlli in accettazione, degli esami iniziali e delle omologazioni necessarie alla messa in esercizio;
- nel caso di acquisti di servizi, anche di natura intellettuale (ad es. acquisto di servizi di progettazione da rendersi a favore della Società o di eventuali clienti), la Società:
  a) subordina l'attività di affidamento alla verifica preliminare delle competenze dei propri fornitori anche sulla base della sussistenza di esperienze pregresse ed eventuali requisiti cogenti (ad es. iscrizione ad albi professionali);
  b) attua il controllo dell'operato dei fornitori attraverso le modalità previste dalle proprie procedure

interne (ad es. procedure di controllo della progettazione cfr. obblighi di vigilanza sui progettisti);

- qualora le attività condotte da detti soggetti possano avere impatti sull'esposizione a rischi per la salute e la sicurezza dei propri lavoratori, attiva preventivamente, tra le altre, le misure di controllo definite ai fini della valutazione dei rischi;
- sono stabilite le modalità di verifica del possesso di idonei requisiti tecnico-professionali del soggetto esecutore delle lavorazioni, anche attraverso la verifica dell'iscrizione alla CCIAA;
- il soggetto esecutore delle lavorazioni dovrà dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di Regolarità Contributiva;
- l'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi rilascia la dichiarazione di conformità alle regole dell'arte;
- con particolare riferimento a fornitori, installatori e manutentori esterni di macchinari, impianti e di qualsiasi tipo di presidio di sicurezza e attrezzature di lavoro da realizzarsi o installare all'interno di pertinenze poste sotto la responsabilità giuridica del datore di lavoro della Società, sono attuati specifici presidi di controllo che prevedono:

  a) individuazione della normativa applicabile (art. 26 o Titolo IV del Testo Unico Sicurezza);

  b) procedure di verifica dei fornitori che tengono conto anche del rispetto da parte degli stessi e dei loro lavoratori delle procedure di sicurezza;

  c) definizione dell'ambito di intervento e degli impatti dello stesso all'interno di in un contratto scritto;

  d) l'indicazione ai predetti soggetti di dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione all'attività della Società;

  e) la definizione degli accessi e delle attività esercitate sul sito da parte dei terzi, con valutazione specifica dei rischi interferenti legati alla loro presenza e relativa redazione della prevista documentazione di coordinamento (ad es. DUVRI, PSC) sottoscritta da tutti i soggetti esterni coinvolti e prontamente adeguata in caso di variazioni nei presupposti dell'intervento;

  f) che il committente e l'appaltatore, o in genere l'esecutore dell'opera o del servizio, cooperano all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto, dell'opera o del servizio. Nel caso in cui il personale dell'appaltatore operi sotto la direzione o il controllo di incaricati della Società, o utilizzando strumenti messi a disposizione da quest'ultima, anche queste fasi dell'attività debbono essere ritenute sensibili, così come la verifica della sicurezza e dell'idoneità dei locali se la prestazione di lavoro viene svolta presso la sede della committente;

  g) clausole contrattuali in merito ad eventuali inadempimenti di lavoratori di terzi presso i siti aziendali relativamente alle tematiche sicurezza, che prevedano l'attivazione di segnalazioni apposite e l'applicazione di penali;

  h) sistemi di rilevamento presenze di lavoratori terzi presso il sito aziendale e di controllo sulle ore di lavoro effettivamente svolte e sul rispetto dei principi di sicurezza aziendali, come integrati eventualmente dai contratti;

  i) la formalizzazione e tracciabilità del controllo da parte dei dirigenti e del datore di lavoro del rispetto dei presidi di controllo sin qui elencati.

Area di rischio: Gestione della Salute e Sicurezza sul Lavoro

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	
Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali.						✔									SSL - Omessa adozione delle misure di prevenzione specificamente previste dalle norme in materia antinfortunistica ed inosservanza dei precetti generali che impongono di esplicare l'attività produttiva in modo che non derivino conseguenze dannose ai prestatori di lavoro.
Gestione della Salute e Sicurezza sul Lavoro.						✔									SSL - Attribuzione di incarichi a soggetti che non possiedono i requisiti tecnico/professionali adeguati rispetto alle funzioni loro delegate e/o alle nomine assegnate.
Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL.						✔									SSL - Sottostimare o sottovalutare i rischi in materia di Salute e Sicurezza sul Lavoro.
Gestione delle emergenze.						✔									SSL - Omessa verifica periodica sull'applicazione ed efficacia delle procedure di emergenza. Omessa informazione e formazione dei lavoratori circa l'attuazione delle procedure di emergenza.
Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.).						✔									SSL - Omessa predisposizione e consegna di procedure operative/istruzioni di lavoro per la conduzione di attività ritenute critiche dal punto di vista della salute e sicurezza sul lavoro.
Sorveglianza sanitaria.						✔									SSL - Affidamento di mansioni comportanti rischi per la salute a lavoratori privi dei necessari requisiti.
Definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori.						✔									SSL - Omessa formazione dei lavoratori subordinati sia sulle misure di prevenzione adottate dalla Società sia sui comportamenti che gli stessi sono tenuti a tenere nello svolgimento delle mansioni affidate.
Comunicazione, partecipazione e consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze.						✔									SSL - Sottostima o sottovalutazione de rischi in materia di Salute e Sicurezza sul Lavoro per la carenza ad es. di comunicazione, coinvolgimento dei lavoratori o delle loro rappresentanze.
Gestione degli incidenti, non conformità e azioni correttive.						✔									SSL - Non adeguata gestione degli incidenti e quasi incidenti e inadeguata identificazione di misure correttive finalizzate ad evitare la successiva esposizione dei lavoratori al rischio SSL.
Approvvigionamento e gestione degli appalti; acquisizione di documentazioni/certificazioni obbligatorie di legge.						✔									SSL - Introdurre attrezzature, macchinari e impianti non conformi ai requisiti normativi ovvero non compatibili con l'ambiente di lavoro.

SEZIONE L – Gestione adempimenti ambientali

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio gestione adempimenti ambientali, ed in particolare alle attività sensibili:

- Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione adempimenti ambientali di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- reati ambientali (art. 25-undecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di gestire gli adempimenti ambientali.

Protocolli specifici di prevenzione

a) Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti.

Per l'attività sensibile gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti, i protocolli prevedono che:

- devono essere richieste e preventivamente acquisite tutte le autorizzazioni, nonché devono essere effettuate le comunicazioni necessarie alla gestione dei rifiuti;
- l'attività di gestione e smaltimento dei rifiuti deve essere svolta con la massima cura ed attenzione con particolare riferimento alla caratterizzazione dei rifiuti, alla gestione dei depositi temporanei, al divieto di miscelazione dei rifiuti siano essi pericolosi o non pericolosi;
- in sede di affidamento delle attività di smaltimento o recupero di rifiuti alle imprese autorizzate deve essere verificata: a) la data di validità dell'autorizzazione, b) la tipologia e la quantità di rifiuti per i quali è stata rilasciata l'autorizzazione ad esercitare attività di smaltimento o recupero; c) la localizzazione dell'impianto di smaltimento e d) il metodo di trattamento o recupero;
- in fase di esecuzione delle attività di trasporto di rifiuti da parte delle imprese autorizzate deve essere verificata: a) la data di validità dell'autorizzazione; b) la tipologia e la targa del mezzo; c) i codici CER autorizzati;
- sono formalizzati ruoli, responsabilità, modalità e controlli nello svolgimento delle attività di conferimento dei rifiuti;

- sono formalizzati controlli sistematici sulle attività di gestione del ciclo dei rifiuti;
- i soggetti coinvolti nell'attività di compilazione e controllo della documentazione inerente i rifiuti ricevono specifica formazione;
- i rifiuti prodotti sono correttamente caratterizzati e classificati e identificati;
- è verificata la congruità del rifiuto prodotto con la qualificazione CER dello stesso, anche qualora il servizio sia eseguito da laboratori terzi;
- le aree dedicate al deposito temporaneo dei rifiuti sono individuate e allestite in conformità alla normativa vigente;
- sono individuate le corrette modalità di deposito temporaneo dei rifiuti sulla base della tipologia e dei quantitativi di rifiuti prodotti;
- le aree di deposito temporaneo sono mantenute pulite e in ordine anche al fine di scongiurare la possibilità che vi sia miscelazione tra rifiuti;
- è prevista la differenziazione dei rifiuti al fine di prevenire ogni illecita miscelazione;
- ciascun rifiuto è chiaramente identificato mediante apposizione all'esterno del relativo contenitore di descrizione e codice identificativo;
- è verificata la congruità dei quantitativi inviati a smaltimento con quelli rappresentati nella documentazione resa;
- è verificata la corretta gestione dei FIR (Formulari di Identificazione dei Rifiuti), anche avvalendosi di *database* e di riepiloghi per codice CER, propedeutico alla corretta compilazione del MUD annuale (Modello Unico di Dichiarazione ambientale);
- è verificata la disponibilità e la corretta archiviazione della documentazione relativa alla gestione dei rifiuti;
- è fatto espresso divieto di:

a) compiere azioni o tenere comportamenti che siano o possano essere interpretati come pratiche volte a danneggiare la salute delle persone e/o le componenti naturali dell'ambiente;

b) conferire l'attività di gestione dei rifiuti a soggetti non dotati di un'apposita autorizzazione per il loro smaltimento e recupero;

c) violare gli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la gestione dei rifiuti;

d) utilizzare impianti e apparecchiature in violazione delle disposizioni normative in materia di sostanze ozono lesive.

Area di rischio: Gestione adempimenti ambientali

Attività sensibili	Categorie di reato													Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	
Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti.								✓							AMB: La Società o soggetti riconducibili alla Società non verificano e monitorano i requisiti dei fornitori (autorizzazioni, iscrizioni agli albi di competenza, ecc.).

SEZIONE M – Attività promozionali, *marketing* e relazioni con il mercato

Premessa

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative all'area di rischio attività promozionali, *marketing* e relazioni con il mercato, ed in particolare alle attività sensibili:

- Attività di *marketing* e promozione del brand;
- Gestione delle informazioni privilegiate e comunicazioni al mercato;
- Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio attività promozionali, *marketing* e relazioni con il mercato di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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 (artt. 24 e 25);
- delitti di criminalità organizzata (art. 24-ter);
- concussione, corruzione, induzione indebita a dare o promettere utilità (art. 25);
- reati societari (art. 25-ter);
- abusi di mercato (art. 25-sexies);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- delitti in materia di violazione del diritto d'autore (art. 25-novies);
- reati transnazionali (art. 10, L. 146/2006);
- reati tributari (art. 25-quinquiesdecies).

Sistema di controllo a presidio del rischio reato

Al fine di mitigare il rischio di commissione dei reati individuati nel paragrafo "Reati applicabili" e di creare un sistema di controllo interno tale da impedire i comportamenti illeciti, la Società ha definito dei protocolli generali applicabili indistintamente a tutte le attività sensibili identificate e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

Tali protocolli trovano definizione anche negli strumenti di attuazione del Modello (procedure, istruzioni operative, ecc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/01, che costituiscono parte integrante dello stesso, così come il corpo procedurale aziendale.

Protocolli generali di prevenzione

Tutti i destinatari del Modello, così come individuati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, ai principi contenuti nel Codice Etico e negli strumenti di attuazione del Modello, al fine di prevenire il verificarsi di reati previsti dal Decreto. Inoltre, all'interno del Codice di Condotta Anti – Corruzione TeamSystem proibisce ogni forma di corruzione a favore di chiunque.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, hanno l'incarico di svolgere le attività promozionali, *marketing* e relazioni con il mercato.

- nessuna donazione o sponsorizzazione può essere promessa, offerta o erogata per assicurare vantaggi commerciali impropri, per fini privati o comunque illeciti. In particolare, non è consentito promettere, proporre, offrire o corrispondere a qualunque titolo contributi, erogazioni o utilità

comunque denominate, anche indirettamente o tramite terze parti, allo scopo di ottenere trattamenti di favore o vantaggi di qualsiasi natura da parte di esponenti della Pubblica Amministrazione, altri pubblici ufficiali o a ricompensarne o influenzarne in qualunque modo l'operato. Anche nei confronti di soggetti privati, è vietato promettere o offrire qualunque donazione, sponsorizzazione o contributo che possa essere interpretato da un osservatore imparziale come diretto ad acquisire vantaggi o trattamenti di favore in modo improprio;

- Tutte le sponsorizzazioni e sonazioni devono essere pagate in modo trasparente e tracciabile;
- Nessuna donazione o sponsorizzazione può essere effettuata in favore di destinatari, sia individui che organizzazioni, i cui scopi sono incompatibili con il Codice Etico, il Codice di Condotta Anti-Corruzione e con il Modello Organizzativo ex D.lgs. 231/2001;
- Nessuna donazione, sponsorizzazione o contributo in favore di enti o associazioni può essere pagato su conti privati di singoli individui;
- I beneficiari delle donazioni e sponsorizzazioni devono sempre essere identificati e devono esserne accertati i requisiti di attendibilità e onorabilità previsti dal Modello Organizzativo e dal Codice di Condotta Anti-Corruzione.

A tale scopo, in nessun caso potrà essere concluso un accordo di sponsorizzazione, erogato un contributo o una Donazione o comunque instaurato un rapporto qualora la controparte:

- rifiuti di sottoscrivere le Clausole 231;
- eserciti la propria attività attraverso strutture o enti "di mera facciata" o "di mero comodo", ovvero privi di una effettiva struttura operativa (ad es. senza essere dotato di organizzazione autonoma di risorse, persone, mezzi, ecc. compatibili rispetto all'impegno dichiarato);
- richieda o proponga: pagamenti, rimborsi, omaggi o altre utilità destinati ad essere rigirati a clienti o a terzi; l'effettuazione di operazioni simulate di qualunque natura; che la propria identità rimanga nascosta; la falsificazione di documenti o attivari; pagamenti in contanti o su conti correnti non intestati all'ente beneficiario della donazione o sponsorizzazione; pagamenti in favore di soggetti diversi da quelli formalmente coinvolti nella transazione; corrispettivi ingiustificati, abnormi o sproporzionati rispetto all'attività svolta.

Inoltre, è fatto divieto di:

- utilizzare di frasi dirette e personali, nel commentare un contenuto condiviso da TeamSystem;
- esprimere commenti o diffondere notizie sui concorrenti TeamSystem e la loro attività, salvo autorizzazione da parte della Direzione *Marketing* and Digital di TeamSystem.

Protocolli specifici di prevenzione

a) Attività di *marketing* e promozione del *brand*.

Per l'attività sensibile di marketing e promozione del brand, i protocolli prevedono che:

- sono adottati strumenti ai fini del monitoraggio delle scadenze dei diritti di utilizzo dei marchi e altri titoli di proprietà intellettuale;
- tutte le attività di comunicazioni relative alla Società sono preventivamente autorizzate;
- prima di condividere notizie attinenti all'attività di TeamSystem il dipendente deve assicurarsi che le stesse non siano riservate e che provengano da fonti interne autorizzate;
- non è consentita la condivisione di materiale (es. audio o video) qualora vi sia la possibilità che tale materiale violi il diritto di autore altrui.

b) Gestione delle informazioni privilegiate e comunicazioni al mercato.

Per l'attività sensibile di gestione delle informazioni privilegiate e comunicazioni al mercato, i protocolli prevedono che:

- devono essere definiti i ruoli e i compiti delle Funzioni e dei Responsabili coinvolti nella predisposizione e divulgazione di dati e notizie all'esterno e deve essere prevista la separazione tra la Funzione fornitrice dei dati, la Funzione incaricata della predisposizione del comunicato e la Funzione/Direzione che autorizza la diffusone dello stesso;
- il soggetto responsabile dell'emissione dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni;
- deve essere previsto un programma di informazione/formazione periodica di amministratori, management e dipendenti delle aree/funzioni aziendali a rischio sulla normativa in materia di abusi di mercato;
- devono esistere procedure autorizzative per acquisti e vendite di strumenti finanziari propri e/o di altre società;
- deve essere predisposto un Registro delle persone che hanno accesso alle informazioni privilegiate;
- deve essere assicurata la riservatezza delle informazioni mediante l'adozione di confidenzialità volte a garantire la sicurezza organizzativa, fisica e logica delle informazioni privilegiate;
- devono essere individuati i soggetti rilevanti e le operazioni da essi effettuate anche per interposta persona con riferimento agli strumenti finanziari della Società;
- sussista l'obbligo di osservare le prescrizioni previste nella procedura aziendale sulla comunicazione all'esterno di informazioni privilegiate;
- sussista l'obbligo di osservare le norme di legge e le regole di funzionamento dei mercati volte a garantire la correttezza dell'informazione;
- non deve essere consentito, attraverso le modalità ritenute più opportune, l'accesso, anche accidentale, alle informazioni privilegiate o destinate a divenire tali da parte di persone diverse da quelle che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, gestiscono e hanno legittimo accesso alle suddette informazioni;
- le informazioni rilevanti comunicate internamente mediante posta elettronica devono essere protette da eventuali rischi di diffusione impropria;
- qualora la Società abbia notizia della diffusione di Informazioni Privilegiate ne deve informare tempestivamente la società emittente;
- sia vietato la comunicazione di informazioni privilegiate relative alla Società tramite canali social anche di natura personale;
- devono essere effettuati e documentati controlli volti a garantire che le informazioni riportate siano:

a) conformi alle norme interne e comunitarie e, in genere, alla normativa applicabile;

b) supportate da adeguata documentazione e/o ricerche scientifiche svolte direttamente dalla Società o da altra Società del Gruppo;

c) essere corrispondenti alla composizione del prodotto per quanto riguarda le caratteristiche qualitative, quantitative e di origine o provenienza;

- devono essere individuati i soggetti cui compete il controllo sulla correttezza e divulgazione delle informazioni e dei soggetti espressamente autorizzati alla diffusione all'esterno di dette notizie;
- devono essere individuate le funzioni aziendali che possono essere chiamate a intrattenere i rapporti con il mercato/ la comunità finanziaria;

- devono essere definite le regole di confidenzialità delle informazioni privilegiate che prevedano espressamente il divieto di diffusione dell'informazione rilevante all'interno o all'esterno della Società, se non tramite il canale istituzionalmente previsto;
- vi sia l'obbligo di osservare le regole di mercato e le raccomandazioni delle Autorità di settore che presiedono alla formazione del prezzo degli strumenti finanziari, evitando condotte idonee a provocarne una sensibile alterazione, tenuto conto della concreta situazione del mercato interessato;
- prima della diffusione del comunicato al pubblico, nessuna dichiarazione o separato comunicato può essere rilasciato o diffuso da parte di esponenti aziendali della Società o delle Società Controllate riguardo ad alcuna Informazione Privilegiata;
- la divulgazione delle Informazioni Privilegiate dovrà essere effettuata secondo modalità che consentano un accesso rapido e una valutazione completa, corretta e tempestiva delle Informazioni Privilegiate, assicurando coerenza e comparabilità con le informazioni già rese note al pubblico, evitando il rischio di asimmetrie informative o il determinarsi di situazioni che possano comunque influire sul prezzo delle Obbligazioni o degli strumenti finanziari derivati collegati. In nessun caso, la divulgazione di Informazioni Privilegiate deve essere coniugata con la commercializzazione delle attività della Società e del Gruppo;
- deve essere identificato un Responsabile del Registro delle persone che hanno accesso alle informazioni privilegiate, avente i compiti di vigilare sulla sua tenuta e sul suo aggiornamento;
- deve essere data evidenza dei motivi di iscrizione di un Amministratore, Dipendente o Collaboratore della Società al suddetto Registro;
- in caso di legittima comunicazione di informazioni privilegiate a soggetti esterni alla Società (ad es., consulenti, società di revisione), siano predisposte clausole contrattuali che vincolano la parte terza alla riservatezza dell'informazione, eventualmente prevedendo l'adozione da parte di tali soggetti di idonee misure di protezione dell'informazione ricevuta;
- devono essere definiti i tempi di comunicazione in materia di Internal Dealing, da parte dei Soggetti Rilevanti e delle Persone Strettamente Associate, agli Enti di competenza ed al Pubblico in linea con le normative vigenti nazionali e internazionali e i regolamenti aziendali;
- è fatto espresso divieto di:

a) diffondere l'informazione rilevante all'interno o all'esterno della Società, se non tramite il canale istituzionalmente previsto;

b) rivelare a terzi informazioni privilegiate relative alla Società, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate ad utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità;

c) concludere operazioni o impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari della Società scendano al di sotto di un certo livello, principalmente per sottrarsi alle conseguenze negative derivanti dal connesso peggioramento del rating degli strumenti finanziari emessi. Questo comportamento deve essere tenuto distinto dalla conclusione di operazioni rientranti nei programmi di acquisto di azioni proprie o nella stabilizzazione degli strumenti finanziari previsti dalla normativa;

d) effettuare, anche a mezzo di terzi, operazioni di acquisto, vendita o di altro tipo su strumenti finanziari negoziati in mercati regolamentati, utilizzando le informazioni privilegiate di cui siano venuti a conoscenza nello svolgimento delle proprie attività;

e) diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo;

f) raccomandare o indurre soggetti terzi a compiere le azioni di cui ai punti precedenti punti, sulla base delle medesime informazioni;

g) ai Soggetti Rilevanti, di compiere le Operazioni per proprio conto o per conto di terzi, direttamente o indirettamente, relative alle Obbligazioni, agli strumenti finanziari derivati o altri strumenti finanziari collegati nel periodo di tempo precedente alla comunicazione al pubblico dei bilanci o delle relazioni finanziarie intermedie che la Società sia tenuta a rendere pubblici, così come previsto dalla normativa vigente.

c) Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità.

Per l'attività sensibile di gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità, i protocolli prevedono che:

- deve esistere una autorizzazione formalizzata a conferire utilità;
- devono esistere documenti giustificativi delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità, validati dal superiore gerarchico e archiviati;
- è prevista la rilevazione di operazioni (donazioni, sponsorizzazioni, omaggi e liberalità) ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette;
- l'inizio della sponsorizzazione deve sempre essere preceduta dalla stipula di un accordo/contratto scritto di sponsorizzazione che specifichi almeno il destinatario della sponsorizzazione, gli obblighi assunti dal soggetto sponsorizzato nei confronti della Società, le relative coordinate bancarie e termini di pagamento, l'esatto ammontare del corrispettivo / contributo, l'evento a cui i fondi sono destinati;
- il contratto deve prevedere specifiche clausole dirette a garantire la corretta attuazione dei principi e delle regole di comportamento previste dal Codice Etico, il Codice di Condotta Anti-Corruzione e dal Modello Organizzativo;
- la controparte ricevente il corrispettivo / contributo deve sempre essere chiaramente identificabile. Deve esservi coincidenza tra controparte formale della transazione (così come risultante dal contratto di sponsorizzazione) ed effettivo destinatario del pagamento;
- nei contratti di sponsorizzazione deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- deve essere verificata la regolarità dei pagamenti per donazioni, sponsorizzazioni o liberalità con riferimento alla piena coincidenza dei destinatari dei pagamenti e le controparti effettivamente coinvolte;
- sono immediatamente interrotte o, comunque, non è data esecuzione ad operazioni relative a donazioni, sponsorizzazioni, omaggi e liberalità, che vedano coinvolti come beneficiari, soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;
- non si possa effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a dipendenti di altre società private;
- non si possa effettuare o promettere, in favore dei clienti, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito;
- nessuna Donazione o Sponsorizzazione può essere effettuata in favore di destinatari, sia individui che organizzazioni, i cui scopi sono incompatibili con il Codice Etico, il Codice di Condotta Anti-Corruzione e con il Modello Organizzativo ex D.lgs. 231/2001;
- l'inizio della prestazione deve sempre essere preceduta dalla stipula di un accordo/contratto scritto di sponsorizzazione che specifichi almeno il destinatario della sponsorizzazione, gli obblighi assunti dal soggetto sponsorizzato nei confronti della società del Gruppo TeamSystem, le relative coordinate bancarie e termini di pagamento, l'esatto ammontare del corrispettivo / contributo, l'evento a cui i fondi sono destinati;

- il Responsabile della Direzione competente autorizza l'erogazione dell'omaggio. Qualora la spesa per l'omaggio non sia stata prevista nel budget della direzione interessata, la richiesta dovrà essere autorizzata dall'Amministratore Delegato della Società o dal CFO.

Area di rischio: Attività promozionali, marketing e relazioni con il mercato

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/CP	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RT	
Attività di marketing e promozione del brand.											✔				✔	DA - La Società utilizza immagini tutelate da diritto d'autore senza averne acquisito i diritti di utilizzo. RT -
Gestione delle informazioni privilegiate e comunicazioni al mercato.										✔						MA - Fornire a terzi informazioni privilegiate o fuorvianti, che possano alterare il prezzo di strumenti finanziari quotati, attraverso i media o le comunicazioni al pubblico in genere.
Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità.	✔	✔	✔				✔								✔	PA - La Società eroga omaggi in favore della Pubblica Amministrazione al fine di ottenere adempimenti favorevoli alla società. SOC/CP - La Società effettua sponsorizzazioni e/o elargire erogazioni liberali in tutto o in parte fittizie per generare provviste da usare per commettere reato di corruzione. RIC - La Società effettua erogazioni liberali o donazioni in tutto o in parte fittizie per riciclare denaro proveniente da attività illecite. CRI/TSN - La Società eroga liberalità o donazioni in favore di enti legati alla criminalità organizzata al fine di ottenere in cambio vantaggi indebiti dall'operato degli stessi. RT - La Società, al fine di evadere le imposte in sui redditi o in materia di IVA, effettua sponsorizzazioni in favore di un ente terzo connivente, registrando a livello contabile e nel bilancio la relativa passività, salvo poi ricevere indietro da tale ente, in tutto o in parte, il denaro versato. RT - Nell'ambito dell'erogazione di donazioni e pagamento di quote associative, attraverso una determinazione artificiosa degli oneri, facendo riferimento a donazioni inesistenti o associazioni non attivate, eventualmente avvalendosi di documenti falsi.