MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

DI

TeamSystem Payments S.r.l.

AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

"*Responsabilità amministrativa della Società*"

REVISIONE	*DATA*	*DESCRIZIONE*	*APPROVAZIONE*
00	**31 – 03 – 2021**	**Prima emissione**	**CDA**
01	**06 – 07 – 2023**	**Aggiornamento**	**CDA**

Indice

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO 1
1 Definizioni 4
2 Premessa 5
3 Il Decreto Legislativo 231/2001 6
I. La Responsabilità Amministrativa degli Enti 6
II. I reati previsti dal Decreto 6
III. Criteri di imputazione della responsabilità dell'Ente 6
IV. Le sanzioni previste dal Decreto 9
V. Condizione esimente della Responsabilità amministrativa 11
VI. Le "Linee Guida" di Confindustria 12
VII. Delitti tentati e delitti commessi all'estero 13
4 Il Modello di Organizzazione, Gestione e Controllo di TeamSystem Payments S.r.l. 14
I. La Società 14
II. Modello di Governance e Sistema dei Controlli Interni 15
III. Finalità del Modello 16
IV. Destinatari 17
V. Struttura del Modello 17
VI. Elementi fondamentali del Modello 18
VII. Codice Etico e Modello 18
VIII. Presupposti del Modello 19
IX. Codice Etico 19
X. Struttura organizzativa 20
XI. Sistema autorizzativo 20
XII. Sistema di controllo di gestione e reporting 20
XIII. Sistema di gestione della qualità e della sicurezza delle informazioni 21
XIV. Procedure manuali e informatiche 21
XV. Modifiche del Modello 21
XVI. Le attività propedeutiche all'adozione del Modello Organizzativo 22
XVII. Passi operativi e metodologia applicata 22
XVIII. Reati rilevanti per TeamSystem Payments S.r.l. 23
XIX. Principi di controllo interno generali e specifici 24
XX. Prestazione di servizi infragruppo 25
XXI. Aggiornamento del Modello 26

XXII. Informazione e formazione del personale *26*
5 Organismo di Vigilanza 28
L'Organismo di Vigilanza e i suoi requisiti *28*
Autonomia e indipendenza *28*
Professionalità *28*
Continuità di azione *28*
Libero accesso *29*
Autonomia di spesa *29*
XXIII. Composizione dell'Organismo di Vigilanza, nomina, revoca, cause di ineleggibilità e didecadenza dei suoi membri *29*
XXIV. L'Organismo di Vigilanza di TeamSystem Payments *30*
XXV. Compiti, Poteri e funzioni dell'Organismo di Vigilanza *30*
XXVI. Reporting dell'Organismo di Vigilanza *32*
XXVII. Whistleblowing *33*
XXVIII. Flussi informativi nei confronti dell'Organismo di Vigilanza *34*
XXIX. Invio di informazioni sulle modifiche dell'organizzazione aziendale all'Organismo di Vigilanza *35*
XXX. Il regolamento dell'Organismo di Vigilanza *36*
XXXI. Archiviazione delle informazioni *36*
6 Sistema sanzionatorio 37
I. Principi generali *37*
II. Destinatari e apparato sanzionatorio e/o risolutivo *37*
III. Misure nei confronti dei destinatari delle segnalazioni ("Whistleblowing") *40*
IV. Misure nei confronti dei soggetti esterni aventi rapporti contrattuali/ commerciali *40*
PARTE SPECIALE 42
SEZIONE A - Gestione dei rapporti con la Pubblica Amministrazione *43*
Premessa *43*
Reati applicabili *43*
Sistema di controllo a presidio del rischio reato *43*
Protocolli generali di prevenzione *43*
Protocolli specifici di prevenzione *44*
SEZIONE B - Gestione delle visite ispettive *51*
Premessa *51*
Reati applicabili *51*
Sistema di controllo a presidio del rischio reato *51*
Protocolli generali di prevenzione *51*

Protocolli specifici di prevenzione 52
SEZIONE C – Selezione, gestione ed assunzione del personale 55
Premessa 55
Reati applicabili 55
Sistema di controllo a presidio del rischio reato 55
Protocolli generali di prevenzione 55
Protocolli specifici di prevenzione 56
SEZIONE D – Gestione dei contenziosi giudiziali e stragiudiziali 61
Premessa 61
Reati applicabili 61
Sistema di controllo a presidio del rischio reato 61
Protocolli generali di prevenzione 61
Protocolli specifici di prevenzione 62
SEZIONE E – Gestione delle attività di amministrazione, finanza e controllo 65
Premessa 65
Reati applicabili 65
Sistema di controllo a presidio del rischio reato 65
Protocolli generali di prevenzione 65
Protocolli specifici di prevenzione 67
SEZIONE F – Gestione delle operazioni straordinarie 75
Premessa 75
Reati applicabili 75
Sistema di controllo a presidio del rischio reato 75
Protocolli generali di prevenzione 75
Protocolli specifici di prevenzione 75
SEZIONE G – Gestione dei sistemi informativi e della sicurezza informatica 79
Premessa 79
Reati applicabili 79
Sistema di controllo a presidio del rischio reato 79
Protocolli generali di prevenzione 79
Protocolli specifici di prevenzione 81
SEZIONE H – Approvvigionamento di beni e servizi 86
Premessa 86
Reati applicabili 86
Sistema di controllo a presidio del rischio reato 86
Protocolli generali di prevenzione 86

Protocolli specifici di prevenzione 87
SEZIONE I – Prestazione dei servizi di pagamento 94
Premessa 94
Reati applicabili 94
Sistema di controllo a presidio del rischio reato 94
Protocolli generali di prevenzione 94
Protocolli specifici di prevenzione 96
SEZIONE J – Gestione delle partnership 101
Premessa 101
Reati applicabili 101
Sistema di controllo a presidio del rischio reato 101
Protocolli generali di prevenzione 101
Protocolli specifici di prevenzione 102
SEZIONE K – Gestione della Salute e Sicurezza sul Lavoro 105
Premessa 105
Reati applicabili 105
Sistema di controllo a presidio del rischio reato 105
Protocolli generali di prevenzione 105
Protocolli specifici di prevenzione 106
SEZIONE L – Gestione adempimenti ambientali 118
Premessa 118
Reati applicabili 118
Sistema di controllo a presidio del rischio reato 118
Protocolli generali di prevenzione 118
Protocolli specifici di prevenzione 118
SEZIONE M – Attività promozionali, marketing e relazioni con il mercato 121
Premessa 121
Reati applicabili 121
Sistema di controllo a presidio del rischio reato 121
Protocolli generali di prevenzione 121
Protocolli specifici di prevenzione 121
SEZIONE N – Gestione degli adempimenti per la prevenzione del riciclaggio e del finanziamento delterrorismo 128
Premessa 128
Reati applicabili 128
Sistema di controllo a presidio del rischio reato 128

Protocolli generali di prevenzione *128*
Protocolli specifici di prevenzione *129*
SEZIONE O – Gestione dei rapporti con soggetti ai quali sono attribuite attività di controllo
Premessa *132*
Reati applicabili *132*
Sistema di controllo a presidio del rischio reato *132*
Protocolli generali di prevenzione *132*
Protocolli specifici di prevenzione *132*
SEZIONE P – Gestione degli adempimenti fiscali *135*
Premessa *135*
Reati applicabili *135*
Sistema di controllo a presidio del rischio reato *135*
Protocolli generali di prevenzione *135*
Protocolli specifici di prevenzione *135*

1 Definizioni

Decreto: il Decreto Legislativo 8 giugno 2001, n. 2311.

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 D. Lgs. 231/2001.

Società: TeamSystem Payments S.r.l.

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 complessonormativo, 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 Payments S.r.l. ("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 04/03/2021.

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 settembre2000 n. 300 – il Decreto Legislativo n. 231, 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 sonocoinvolti 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 unregime di responsabilità amministrativa a carico di enti (società, associazioni, etc. di seguito denominati "Enti") per alcuni reati commessi, nell'interesse o vantaggio degli stessida:

- 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 nelfatto 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 contestarel'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 privaticoncessionari 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 dellaresponsabilità all'Ente sono "oggettivi" e "soggettivi".

I criteri di natura ***oggettiva*** prevedono che gli Enti possono essere considerati responsabili ogniqualvolta sirealizzino i comportamenti illeciti tassativamente elencati nel Decreto purché:

- il reato sia stato commesso **nell'interesse** o **a vantaggio** dell'Ente;
- il reato sia stato commesso:
  - "*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"**);
  - "*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'Entesia 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 odi 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 potràessere ritenuta responsabile per il Reato commesso nell'attività della controllata qualora sia ravvisabile ancheun 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, purchéconsapevoli 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.

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

[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.

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'art. 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'art. 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 ("**D. Lgs. 81/2008**"),, 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, agentichimici, 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 sicurezzada 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 e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinareidoneo a sanzionare il mancato rispetto delle misure indicate nel Modello. Il Modello deve altresì prevedere unidoneo 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;

[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.

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, manonanche 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 seguentisanzioni 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 numeronon inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 ad un massimodi 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 statocommesso 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 enon 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

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

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 provocareun 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 prosecuzionedell'attività dell'ente da parte di un commissario, indicandone i compiti e i poteri con particolare riferimento allaspecifica 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 essereapplicate 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 diun certo rilievo ed è già stato condannato, almeno tre volte negli ultimi sette anni, all'interdizione temporaneadall'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 efficaceadeguati 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 da 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 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;

[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).

- 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. 81/2008, secondo cui il Modello 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 sopradescritte, 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 del giugno 2021.

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 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;
- non si procede nei confronti dell'Ente nello Stato in cui è stato commesso il fatto.

[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).

4 Il Modello di Organizzazione, Gestione e Controllo di TeamSystem Payments S.r.l.

I. La Società

TEAMSYSTEM PAYMENTS S.R.L. è una società costituita a Pesaro in data 14 maggio 2019 e successivamente iscritta nel registro delle imprese di Milano.

Ai sensi del combinato disposto dell'art. 1, comma 2, lett. h-septies, ad esempio, 1) e dell'art. 114 sexies del D. Lgs. n. 385 del 1° settembre 1993 ("TUB"), la Società è stata autorizzata quale istituto di pagamento al fine di prestare i seguenti servizi di pagamento:

- esecuzione di operazioni di pagamento, incluso il trasferimento di fondi su un conto di pagamento presso il prestatore di servizi di pagamento dell'utilizzatore o presso un altro prestatore di servizi di pagamento:
  - esecuzione di addebiti diretti, inclusi gli addebiti diretti una tantum;
  - esecuzione di operazioni di pagamento mediante carte di pagamento o dispositivi analoghi;
- servizi di disposizione di ordini di pagamento ("PIS");
- servizi di informazione sui conti ("AIS").

TeamSystem Payments S.r.l. appartiene al Gruppo TeamSystem essendo indirettamente controllata dalla principale società operativa del gruppo, TeamSystem S.p.A., a sua volta controllata al 100% dalla holding capogruppo TeamSystem Holding S.p.A.. In particolare, TeamSystem S.p.A. è stata costituita nel 1979 ed è oggi un'azienda leader sul mercato italiano per quanto attiene alle soluzioni digitali per la gestione del business delle micro, piccole e medie imprese italiane di ogni settore, dei professionisti e delle associazioni di ogni genere.

La Società, si propone di affiancare i professionisti e le micro, piccole e medie imprese con il fine ultimo di efficientare e migliorare i servizi di incasso e pagamento. In dettaglio, il principale obiettivo perseguito dalla Società è quello di incrementare i servizi digitali e fintech messi a disposizione dal Gruppo TeamSystem alla propria clientela con l'intento di digitalizzare anche la filiera dei pagamenti e degli incassi, garantendo l'accesso ad un sistema semplice, efficace, trasparente e sicuro.

Sebbene in via autonoma e indipendente rispetto ai servizi offerti da TeamSystem S.p.A., la Società intende in prima battuta rivolgersi al suo ampio bacino di clienti offrendo agli utenti un servizio di pagamento principalmente focalizzato sulla gestione degli incassi che andrebbe ad integrarsi perfettamente con il software gestionale già in uso da parte della clientela afferente al Gruppo TeamSystem.

La mission imprenditoriale della Società è quella di fornire ai propri clienti un servizio di pagamento innovativo che permetta una gestione degli incassi e dei pagamenti completamente digitale e integrata con gli altri sistemi informatici già in uso presso i clienti.

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 e 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 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 e 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. 231/2001.

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 e Sistema dei Controlli Interni

1. 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.

2. Sistema dei Controlli Interni

Il Sistema dei Controlli Interni riveste un ruolo centrale nell'organizzazione della Società, in particolare:

- rappresenta un elemento fondamentale di conoscenza per gli organi societari in modo da garantire piena consapevolezza della situazione ed efficace presidio dei rischi della Società e delle loro interrelazioni;
- orienta i mutamenti delle linee strategiche e delle politiche societarie e consente di adattare in modo coerente il contesto organizzativo;
- presidia la funzionalità dei sistemi gestionali;
- favorisce la diffusione di una corretta cultura dei rischi, della legalità e dei valori societari. La Società attribuisce un rilievo strategico al Sistema dei Controlli Interni, in quanto considera lo stesso come elemento fondamentale per garantire la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi e delle operazioni societarie, l'affidabilità dell'informazione finanziaria, il rispetto di leggi e regolamenti.

Il Sistema dei Controlli Interni della Società, in conformità con quanto previsto dalle "Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica della Banca d'Italia", è così strutturato:

- **revisione interna** (i.e. controlli di terzo livello), volta a individuare andamenti anomali, violazione delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, della funzionalità e dell'adeguatezza del Sistema dei Controlli Interni, inclusi quelli sul sistema informativo, con cadenza prefissata in relazione alla natura e all'intensità dei rischi. L'attività è condotta da una funzione diversa e indipendente dalle funzioni operative (cd. Funzione di Internal Audit), anche attraverso verifiche in loco;
- **controlli sulla gestione dei rischi e di conformità alle norme** (i.e. controlli di secondo livello), che hanno l'obiettivo di concorrere alla definizione delle metodologie di misurazione dei rischi, di verificare il rispetto dei limiti assegnati alle varie funzioni operative e di controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio-rendimento assegnati, nonché alle norme dell'operatività. Essi sono affidati a strutture diverse da quelle operative e, nello specifico, alla Funzione Compliance & Risk Management. Le funzioni di controllo concorrono alla definizione delle politiche di governo e del processo di gestione dei rischi aziendali;
- **controlli di linea** (i.e. controlli di primo livello), diretti ad assicurare il corretto svolgimento delle operazioni connesse con la prestazione dei servizi di pagamento. Essi sono effettuati dalle unità organizzative della Società, quali prime responsabili del processo di gestione dei rischi, essendo le stesse chiamate, nel corso dell'operatività giornaliera, a identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività societaria, in conformità con il processo di gestione dei rischi.

Ai sensi della "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo" adottate con provvedimento della Banca d'Italia, la Società ha altresì istituito una Funzione Antiriciclaggio.

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 estrumenti 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 esserecommessi 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 sistemadi 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 diattività 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 edell'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. 231/2001, 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.

È 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. Cionondimeno, 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

[7] Tramite l'analisi documentale e le interviste svolte, con i soggetti aziendali informati dell'organizzazione e delle attività svolte dalle Funzioni/Aree, 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.

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:

- 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, 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:

a) verificabilità, documentabilità, coerenza e congruità di ogni operazione;
b) separazione delle funzioni coinvolte nella gestione di ciascun processo;
c) chiara definizione e formalizzazione delle responsabilità e dei poteri attribuiti dalla Società;
d) necessità che ciascuna operazione significativa trovi origine in un'adeguata autorizzazione interna;
e) previsione di limiti all'esercizio di poteri in nome e per conto della Società;
f) coerenza tra i poteri formalmente conferiti e quelli concretamente esercitati nell'ambito dell'organizzazione della Società;
g) 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;
h) documentazione e documentabilità dei controlli effettuati.

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 ambiguiattraverso una chiara enunciazione delle regole da rispettare, con l'avvertenza che in caso di violazione i destinatari potranno essere sanzionati.

La Società, nel perseguimento della propria attività, si impegna, in particolare, nel contrasto alla corruzione e nella prevenzione dei rischi di pratiche illecite, a qualsiasi livello lavorativo, sia attraverso la diffusione e la promozione di valori e principi etici, sia mediante l'effettiva previsione di regole di condotta e l'effettiva attuazione di processi di controllo, in linea con i requisiti fissati dalle normative applicabili e con le migliori pratiche internazionali. A tale riguardo TeamSystem ha adottato un Codice di condotta che rappresenta un sistema di regole ispirate a principi di integrità e trasparenza, volto a contrastare i rischi di pratiche illecite nella conduzionedegli affari e delle attività aziendali.

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/ Funzioni 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 e 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 edivulgato a tutti i livelli tramite gli strumenti informativi aziendali.

XI. Sistema autorizzativo

La Società ha adottato un sistema 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'internodell'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 e le responsabilità organizzative e gestionali effettivamente assegnate all'internodell'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 (ad esempio, variazioni di responsabilità o attribuzione di nuove competenze), così come in casodi 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.

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 avvale del supporto di TeamSystem S.p.A., parte del Gruppo TeamSystem, alla quale sono stati esternalizzati alcuni servizi informativi e informatici. A tale proposito si evidenzia che TeamSystem S.p.A. si è dotata di un sistema organizzativo e gestionale che soddisfa i seguenti standard internazionali:

- la norma UNI EN ISO 9001:2008 in materia di qualità del prodotto;
- 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 progammata, 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 e informatiche

L'attività della Società è regolata da una serie di policies e procedure, manuali e 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:

- "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;
- "progettazione del sistema di controllo" (c.d. protocolli per la programmazione della formazione ed attuazione della 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 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:

- 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 nell'ambito della redazione del Modello Organizzativo adottato in data 4 marzo 2021. Le attività svolte sono descritte nel documento "*Risk Self Assessment*", che viene conservato agli atti della società.

XVIII. Reati rilevanti per TeamSystem Payments S.r.l.

Sulla base dell'analisi condotta i reati potenzialmente realizzabili nel contesto aziendale della Società sono i seguenti:

- indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea oper il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato di un ente pubblico e frode nelle pubbliche forniture (art. 24);
- delitti informatici e trattamento illecito di dati (art. 24-bis);
- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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 con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater);
- 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 tributari (art. 25-quinquiesdecies);
- reati transnazionali (art. 10, L. 146/2006).
- reati effettuati con strumenti di pagamento diversi dai contanti (art. 25-octies.1).
- delitti contro il patrimonio culturale (25-septiesdecies).
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (25-duodeviecies).

Il rischio di commissione dei reati di cui agli artt., 25-bis.1 "Delitti contro l'industria e il commercio", 25-quarter.1"Pratiche di mutilazione degli organi genitali femminili", 25-terdecies "Razzismo e Xenofobia", 25-quaterdecies "Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati", 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.

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.
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. Prestazione dei servizi di pagamento.
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
N. Gestione degli adempimenti per la prevenzione del riciclaggio e del finanziamento del terrorismo
O. Gestione dei rapporti con soggetti ai quali sono attribuite attività di controllo
P. Gestione degli adempimenti fiscali.

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 svolgimentodelle 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 incaricatidella 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 elaboranoevidenza 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 specificoambito di operatività della delega;
  - l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguenteassunzione 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 controllioperativi 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 datiin 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, conmodalità 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 adaltri organi di controllo interno, alla società di revisione eventualmente nominata e all'Organismo di Vigilanza.

XX. 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 Etico e del Modello, nonché le disposizioni del D. Lgs. 231/2001 e di operare in linea con essi.

XXI. 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.

XXII. Informazione e formazione del personale

È obiettivo generale di TeamSystem 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 su 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 dalla Direzione 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 ex D. Lgs. 231/2001, 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 Risorse Umane.

5 Organismo di Vigilanza

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 D. Lgs. 231/2001 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 principali caratteristiche di seguito riportate.

Autonomia e indipendenza

I requisiti di autonomia e 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 (ad esempio, modalità di convocazione delle riunioni, documentazione dell'attività, etc.).

Si precisa, infine, che la Legge n. 183 del 2011 (cd. 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.

XXIII. 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 sono stabiliti 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'art. 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, comma1, 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.

XXIV. L'Organismo di Vigilanza di TeamSystem Payments

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 collegiale (OdV) e alla nomina dei suoi componenti.

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.

XXV. 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 illecitiprevisti dal Decreto;
- vigilanza sulla corretta applicazione del Sistema Disciplinare da parte delle funzioni aziendali allostesso 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 delModello;
- 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, iviincluso 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 necessariemodifiche 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" (ad esempio, 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 delDecreto 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 diseguito 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 attribuiteall'OdV, ivi inclusi i libri societari di cui all'art. 2421 del Codice Civile;
- 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 altrefunzioni 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 delegarepredefiniti 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.

XXVI. 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 di Amministrazione, al quale dovrà essere trasmessa una relazione scrittaavente 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,

- le sanzioni disciplinari (connesse con comportamenti rilevanti ai fini del Decreto) eventualmenteirrogate dai soggetti competenti;
- le criticità emerse in relazione al Modello e 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 di 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.

XXVII. Whistleblowing

Il Decreto Legislativo 10 marzo 2023, n. 2023, 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, contrarie 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 TeamSystem Payments - Speak UP!. 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.

XXVIII. 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 "Responsabile di Area" che dovranno, tra l'altro, fornire all'OdV i flussi informativi secondo le modalità e con la frequenza definite in uno specifico "*Protocollo per la gestione dei flussi informativi verso l'organismo di vigilanza*", 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, del Codice Etico o del Codice di Condotta Anticorruzione, ovvero fattispecie di reato.

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

organismodivigilanzatspay@teamsystem.com

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

TeamSystem Payments S.r.l., Att.ne Organo di Vigilanza,

Via Emilio Cornalia 11 - 20124 Milano

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. Analogamente, saranno esaminate dall'Organismo di Vigilanza le segnalazioni pervenute attraverso la Piattaforma di Whistleblowing secondo le modalità previste nella Policy di riferimento.

Sebbene siano da preferirsi le segnalazioni in cui sia indicato il nominativo del segnalante, l'Organismo di Vigilanza prenderà in considerazione anche segnalazioni anonime purché dal contenuto sufficientemente preciso e circostanziato. Non saranno tenute in considerazione segnalazioni dal contenuto generico ovvero palesemente diffamatorio.

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, eventiod omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o del Modello;
- significative modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche di rilievo dell'organigramma aziendale;
- procedimenti disciplinari avviati in relazione alla violazione del Codice Etico o del Modello Organizzativo erelativi esiti (anche in caso di archiviazione);
- segnalazione di infortuni gravi (in ogni caso qualsiasi infortunio con prognosi superiore ai quaranta (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 dallerichieste 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 messia disposizione della Società, sia ogni altra situazione di pericolo connesso alla tutela dell'ambiente e della salute e sicurezza sul lavoro.

Si rinvia al "*Protocollo per la gestione dei flussi informativi verso l'organismo di vigilanza*", allegato al Modello,per la completa formalizzazione dei flussi/ segnalazioni in discorso.

XXIX. 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 alleattività a rischio di commissione reato ed alla luce dell'assetto organizzativo adottato dalla Società, iResponsabili 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, etc.);
- gli aggiornamenti e i mutamenti significativi 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 emerganomodifiche 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 esempio, Autorità Garante perla 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.

XXX. 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.

XXXI. Archiviazione delle informazioni

Di tutte le richieste, le consultazioni e le riunioni tra l'OdV e le altre funzioni aziendali, l'Organismo di Vigilanzaha 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, 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 e, 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, 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'art. 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 esempioil 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 disciplinariper i Dipendenti:

- richiamo verbale;
- ammonizione scritta;
- multa in misura non eccedente l'importo di quattro (4) ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di dieci (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 cinque (5) giorni da tale contestazione, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.Se il provvedimento non verrà emanato entro i cinque (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 sei (6) giorni dalla contestazione dell'illecito anche nel caso in cui il dipendentenon 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 ilperiodo 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 previstedai CCNL di riferimento. Non si terrà conto delle sanzioni trascorsi due (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 Modellostesso, 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 cheverbale; tenutoconto della gravità delcomportamento e delle mansioni svolte dal lavoratore, potrà esserecomminata 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, etc.).

— 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 esempio, 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 (o Comitato Whistleblowing)***

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. 231/2001 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 e Codice di Condotta Anticorruzione);
- 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 e dal Codice di Condotta Anticorruzione, nonché dal corpo procedurale e documentale della Società, al fine di prevenire la commissione dei reati contemplati nel D. Lgs.231/2001.

SEZIONE A - Gestione dei rapporti con la Pubblica Amministrazione

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 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 (ad esempio, Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni);
- Gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (ad esempio, Garante Privacy, Antitrust, Agenzia delle Entrate, etc.) 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 (ad esempio, Registro delle imprese presso le Camere di Commercio competenti);
- Gestione dei rapporti con e degli obblighi verso le Autorità di Vigilanza - Banca d'Italia (ad esempio, comunicazioni da e verso le Autorità, invio delle Segnalazioni di Vigilanza, Segnalazioni Or.So.).

Reati applicabili

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

- indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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) influenzare in alcun modo le decisioni di rappresentanti della Pubblica Amministrazione in maniera impropria e/o illecita (come, a titolo di esempio, sollecitare e/o accettare e/o corrispondere e/o offrire ai medesimi, direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altrivantaggi per sé o per la Società). Atti di cortesia commerciale (come, a titolo di esempio, omaggi o formedi ospitalità) sono consentiti solo se non eccedono le normali pratiche commerciali e/o di cortesia e se, in ogni caso, sono tali da non compromettere l'imparzialità e l'indipendenza di giudizio del rappresentante della 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.

La Società, inoltre, vieta di:

- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, unvantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva);

quando l'intenzione sia di:

- indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di naturapubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
- influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;
- influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

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 (ad esempio, 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 Soggettiappartenenti a Enti Pubblici di rilevanza nazionale e locale (adesempio, 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;
- tutti gli incontri rilevanti con il rappresentante della Pubblica Amministrazione devono essere riportati all'interno di un registro predisposto con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, etc.;

- 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 Area/ Funzione 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 inviata, a cura dei Responsabili della Area/ Funzione, secondo le richieste dall'OdV, un'analisi delle transazioni con la Pubblica Amministrazione e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività;
- 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.

b) Gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (Autorità Garante della Concorrenza e del mercato, Ufficio Brevetti, Garante Privacy, Antitrust, etc.) 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 (a desempio, Garante Privacy, Antitrust, Agenzia delle Entrate, etc.) e gestione delle comunicazioni e delle informazioni a esse dirette 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;
- tutti gli incontri rilevanti con il rappresentante della Pubblica Amministrazione devono essere riportati all'interno di un registro predisposto con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, etc.;
- 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 Area/ Funzione 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;
- deve essere inviata, a cura dei Responsabili della Area/ Funzione, secondo le richieste dall'OdV, un'analisi delle transazioni con la Pubblica Amministrazione e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività;
- 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, etc.) 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;
- è fatto divieto di 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;
- è fatto divieto di esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;

- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione degli adempimenti versol'Agenzia delle Entrate;
- la Società, per quanto riguarda gli adempimenti verso l'Agenzia delle Entrate, si impegna a trasmettere tutti i dati e le informazioni che riguardano le tematiche riportate in merito ai servizi erogati dalla stessa nella normativa interna di riferimento.

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:

- è fatto espresso divieto di:
  - indurre taluno in errore utilizzando artifici o raggiri a i 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 leggee della corretta pratica commerciale a fronte di trattative, concessioni, licenze, etc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;
  - utilizzare o presentare dichiarazioni o documenti falsi, ovvero omettere informazioni dovute per l'ottenimento di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concesse o erogate dallo Stato, da altri enti pubblici o dall'Unione Europea;
  - destinare a uso diverso un finanziamento ottenuto dallo Stato, o da altro ente pubblico o dall'Unione Europea;
  - procurare indebitamente qualsiasi altro tipo di profitto (licenze, autorizzazioni, sgravi di oneri, anche previdenziali, etc.) con mezzi che costituiscano artifici o raggiri (per esempio invio di documentazione non veritiera);
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono gestiti esclusivamente dai soggettiaziendali muniti di idonei poteri in conformità al sistema di deleghe e procure, ovvero da coloro che sianoda 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;
- tutti gli incontri rilevanti con il rappresentante della Pubblica Amministrazione devono essere riportati all'interno di un registro predisposto con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, etc.;
- 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 Area/ Funzione 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;
- deve essere inviata, a cura dei Responsabili della Area/ Funzione, secondo le richieste dall'OdV., un'analisi delle transazioni con la Pubblica Amministrazione e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività;
- 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, etc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- deve essere effettuata 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;
- devono essere definiti chiaramente i ruoli e le responsabilità operative con riferimento alla gestione dei finanziamenti pubblici;
- deve essere effettuato un continuo monitoraggio, supportato da evidenze formali, circa il corretto utilizzo dei fondi/ finanziamenti ricevuti rispetto agli scopi cui erano destinati;
- deve essere effettuato un monitoraggio della normativa di riferimento e deve provvedersi all'archiviazione della documentazione;
- 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;
- 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.

d) Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (ad esempio, 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 (ad esempio, Registro delle imprese presso le Camere di Commercio competenti), i protocolli prevedono che:

- 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;
- tutti gli incontri rilevanti con il rappresentante della Pubblica Amministrazione devono essere riportati all'interno di un registro predisposto con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, etc.;
- tutta la documentazione deve essere autorizzata e sottoscritta da parte del responsabile dell'Area/ Funzione o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna Area/ Funzione 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,fomendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- deve essere inviata, a cura dei Responsabili dell'Area/ Funzione, secondo le richieste dall'OdV, un'analisidelle transazioni con la Pubblica Amministrazione. e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività;
- 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, etc.) 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 conflitti di interesse.

e) Gestione dei rapporti con e degli obblighi verso le Autorità di Vigilanza - Banca d'Italia (ad esempio, comunicazioni da e verso le Autorità, invio delle Segnalazioni di Vigilanza, Segnalazioni Or.So.).

Per l'attività sensibile Gestione dei rapporti con e degli obblighi verso le Autorità di Vigilanza - Banca d'Italia (ad esempio, comunicazioni da e verso le Autorità, invio delle Segnalazioni di Vigilanza, Segnalazioni Or.So.),i protocolli prevedono che:

- 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 sia noda 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;
- tutti gli incontri rilevanti con il rappresentante della Pubblica Amministrazione devono essere riportati all'interno di un registro predisposto con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, etc.;
- tutta la documentazione deve essere autorizzata e sottoscritta da parte del Responsabile della Area/ Funzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della Società;
- ciascuna Area/ Funzione 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,fomendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- deve essere inviata, a cura dei Responsabili della Area/ Funzione secondo le richieste dall'OdV, un'analisi delle transazioni con la Pubblica Amministrazione e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività;
- 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, etc.) 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 conflitti di interesse;

- la Società ha definito ruoli e responsabilità, un iter operativo e un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti (ad esempio, segnalazioni alla Banca d'Italia);
- l' Area Amministrazione, Finanza e Controllo, una volta confermata la ricezione dei dati inviati ufficialmente,qualora non vi siano rilievi/ nuovi rilievi da notificare da parte della Banca d'Italia, provvede a mantenerneprova e ne stampa le evidenze dal portale Banca d'Italia. Successivamente tali evidenze vengono opportunamente archiviate in formato elettronico;
- la Società ha definito i compiti e le attività dei soggetti coinvolti a vario titolo nel processo adottato per il trattamento dei reclami, inerenti alla prestazione dei servizi di pagamento, presentati dai Clienti;
- la Società ha definito i compiti e le attività dei soggetti coinvolti a vario titolo nell'evasione delle pratiche relative al riscorso all'Arbitro Bancario Finanziario;
- in caso di rimborsi, il Responsabile della gestione dei reclami verifica che la registrazione/ archiviazione della documentazione prodotta e il pagamento del rimborso siano avvenuti nel rispetto delle regole;
- tutti i reclami presentati dai clienti vengono inseriti in un apposito registro ("Registro dei Reclami") a cura dell'Ufficio Reclami che procederà all'aggiornamento periodico e all'archiviazione, con tracciamento dell'attività di istruttoria e storicizzazione di tutte le risposte fornite;
- il nominativo del Responsabile della gestione dei reclami deve essere comunicato alla Banca d'Italia;
- il Consiglio di Amministrazione, con cadenza almeno annuale, esamina le relazioni relative all'attività svolta dal responsabile antiriciclaggio e ai controlli eseguiti dalle funzioni competenti, nonché il documento sui risultati dell'autovalutazione dei rischi di riciclaggio e ne assicura la trasmissione alla Banca d'Italia;
- la Società entro 20 giorni dalla delibera consiliare di nomina o di revoca del Responsabile della Funzione Antiriciclaggio ne dà comunicazione alla Banca d'Italia;
- la Funzione Antiriciclaggio conduce l'esercizio annuale di autovalutazione dei rischi di riciclaggio, ne presenta i risultati al Consiglio di Amministrazione e al Collegio Sindacale. Successivamente la Società trasmette alla Banca d'Italia entro il 30 aprile di ciascun anno, la relazione della funzione antiriciclaggio, che include l'esercizio di autovalutazione del rischio;
- i componenti dell'organo con funzione di controllo comunicano senza ritardo alla Banca d'Italia tutti i fatti di cui vengano a conoscenza nell'esercizio delle proprie funzioni che possano integrare violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge applicabili e delle relative disposizioni attuative.

Area di rischio: Gestione dei rapporti con la Pubblica Amministrazione.

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (ad esempio, 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 indebiti vantaggi.
Gestione di rapporti con i Funzionari pubblici, le Autorità Amministrative Indipendenti (Autorità Garante della Concorrenza e del mercato, Ufficio Brevetti, Garante Privacy, Antitrust, etc.) 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.

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 (ad esempio, Registro delle imprese presso le Camere di Commercio competenti).	✔															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 (ad esempio, mancata denuncia/comunicazione al Registro delle Imprese di operazioni finanziarie)
Gestione dei rapporti con e degli obblighi verso le Autorità di Vigilanza - Banca d'Italia (ad esempio, comunicazioni da e verso le Autorità, invio delle Segnalazioni di Vigilanza, Segnalazioni Or.So.).	✔	✔														PA - La Società condiziona indebitamente pubblici ufficiali delle Autorità di Vigilanza al fine di ottenere l'accelerazione di pratiche in corso. SOC/CP – La Società omette fatti o comunica fatti non veritieri alle Autorità di Vigilanza (ad esempio, alimentazione AUI).

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 e delle Autorità Amministrative Indipendenti, in particolare delle Autorità di Vigilanza (Banca d'Italia, Garante Privacy), 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:

- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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 tributari (art. 25-quinquiesdecies);
- reati transnazionali (art. 10, L. 146/2006).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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) influenzare in alcun modo le decisioni di rappresentanti della Pubblica Amministrazione in maniera impropria e/o illecita (come, a titolo di esempio, sollecitare e/o accettare e/o corrispondere e/o offrire ai medesimi, direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per sé o per la Società). Atti di cortesia commerciale (come, a titolo di esempio, omaggi o forme di ospitalità) sono consentiti solo se non eccedono le normali pratiche commerciali e/o di cortesia e se, in ogni caso, sono tali da non compromettere l'imparzialità e l'indipendenza di giudizio del rappresentante

   della 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) in occasione di un procedimento giudiziario e/o di un'indagine/ispezione da parte delle Autorità pubbliche:

- distruggere/alterare registrazioni, verbali, scritture contabili e qualsiasi altro tipo di documento,
- mentire o fare/intimare a fare dichiarazioni false alle autorità competenti;

qualsiasi tentativo di estorsione o di concussione da parte di un pubblico ufficiale devono essere segnalati al proprio Responsabile.

La Società, inoltre, vieta di:

- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva); quando

l'intenzione sia:

- indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di natura pubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
- influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;
- influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

Protocolli specifici di prevenzione

a) Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti 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:

- 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;
- tutti gli incontri rilevanti con il rappresentante della Pubblica Amministrazione devono essere riportati all'interno di un registro predisposto con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, etc.;
- i funzionari della Pubblica Amministrazione devono essere accompagnati durante le verifiche ispettive da almeno due rappresentanti della Società;
- tutta la documentazione deve essere verificata e sottoscritta da parte del responsabile dell'Area/ Funzione o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;

- ciascuna Area/ Funzione 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 inviata, a cura dei Responsabili della Area/ Funzione, secondo le richieste dall'OdV, un'analisi delle transazioni con la Pubblica Amministrazione e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività;
- 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, etc.) 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;
- 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;
- 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; l'eventuale volontà di firmare è apposta dal delegato della Società;
- è compito del Responsabile dell'Area/ Funzione interessata dalla visita ispettiva, dopo aver accertato l'oggetto dell'ispezione, individuare le risorse deputate a gestire i rapporti con i Funzionari pubblici durante la loro permanenza presso la Società. Le Funzioni di Controllo e, nei casi particolarmente rilevanti, l'Organismo di Vigilanza devono essere tempestivamente informate della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall'Autorità;
- è fatto divieto di occultare o distruggere in tutto o in parte e scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari della Società durante lo svolgimento delle visite ispettive;
- la Società ha definito un iter operativo e ruoli e responsabilità per quanto riguarda la gestione delle visite ispettive (ad esempio, visita ispettiva da parte della Banca d'Italia);
- una volta avviata l'ispezione l'Amministratore Delegato informa il/i responsabile/i della/e unità organizzativa/e oggetto dell'ispezione. Per la gestione della visita ispettiva, inoltre, è necessario il coinvolgimento delle seguenti funzioni: Compliance, Risk Management, Internal Audit, Antiriciclaggio e Legal, nonché di quelle di volta in volta interessate;
- le unità organizzative interessate dell'ispezione devono provvedere tempestivamente alla raccolta della documentazione e delle informazioni richieste dall'Autorità Ispettiva, con l'eventuale coinvolgimento di altre funzioni interne interessate;
- ricevuta la comunicazione, il Responsabile della Unità Organizzativa oggetto dell'ispezione provvede a fornire con tempestività e completezza i documenti e/o gli accessi di rete che gli incaricati ritengono necessario acquisire. Nel caso in cui le informazioni richieste non siano di competenza della struttura, informa la Funzione responsabile che provvede alla raccolta tempestiva delle informazioni richieste;
- lo svolgimento di una visita ispettiva deve essere opportunamente riportato nel registro delle Verifiche Ispettive dalla Funzione Compliance e Risk Management;
- una volta conclusa l'ispezione la struttura aziendale oggetto di ispezione deve predisporre, con il supporto di strutture interne, opportuna relazione contenente la lista completa della documentazione richiesta e fornita e i relativi controlli effettuati dall'Autorità. La relazione è rivista dal Responsabile Compliance e Risk Management e approvata dall'Amministratore Delegato approva la relazione, che è incaricato di inviarla all'Autorità Ispettiva e aggiornare prontamente il Consiglio di Amministrazione;

- nell'ambito delle ispezioni dell'Autorità Garante per la Privacy, tutti i soggetti interessati agli accertamenti sono tenuti a norma di legge a farli eseguire e devono prestare la collaborazione necessaria per consentire l'esecuzione dell'accertamento. È fatto, altresì, obbligo di:
  - dimostrarsi sempre collaborativi, ma – finché non è presente un Delegato della Società – comunicare che non si è nella posizione di rilasciare dichiarazioni e di dar seguito alle richieste e che occorre attendere le persone appropriate;
  - dare seguito alla richiesta dell'Autorità e non rifiutare mai l'accesso
  - per il Data Protection Officer e/o i Delegati Principali della Società e i Referenti Privacy competenti, presenziare durante tutto il corso delle operazioni, assistendo i colleghi che potrebbero essere convocati dall'Autorità e verificando che gli stessi adottino le precauzioni che seguono;
  - dare seguito alle richieste dell'Autorità Garante per la Privacy, esibendo i documenti richiesti e rispondendo alle richieste di informazioni, ma limitando le risposte a quanto rilevante rispetto all'oggetto dell'indagine;
  - rilasciare sempre informazioni complete e veritiere. Eventuali omissioni potrebbero comportare accertamenti ulteriori e più invasivi dell'Autorità. Qualora non si sia a conoscenza della risposta, semplicemente comunicarlo ai funzionari del Garante;
  - consentire ai funzionari di effettuare accessi ad archivi e database dove sono trattati i dati indicando quelli rilevanti rispetto all'oggetto delle indagini;
  - consentire ai funzionari di effettuare rilievi, fare fotocopie, copiare file, etc.;
  - non rilasciare mai documenti originali, ma solo copie di documenti e verificare che queste copie vengano custodite dai funzionari dell'Autorità in maniera appropriata (ad esempio, inseriti in apposite cartelline, chiavette USB criptate, etc.);
  - prendere nota di tutti i documenti che vengono visionati dall'Autorità e delle informazioni richieste;
  - in caso di richiesta di documenti riservati (ad esempio, documenti coperti da un accordo di riservatezza con un'altra società) assicurarsi di far visionare e prendere copia solo degli elementi rilevanti;
  - anche se si ha certezza sulle risposte fornite, riservarsi sempre di produrre ulteriori informazioni e/o documenti, chiedendo appositamente che tale riserva sia segnata a verbale;
  - assicurarsi sempre che ogni elemento che si ritiene utile, sia segnato a verbale dai funzionari;
  - all'esito delle operazioni, farsi rilasciare una copia del verbale;
  - se il Data Protection Officer non è intervenuto durante le operazioni, informarlo il prima possibile riguardo alle operazioni.

Area di rischio: Gestione delle visite ispettive.

Attività sensibili	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	Esempi di reato
Gestione dei rapporti con i Funzionari della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti, in particolare delle Autorità di Vigilanza (Banca d'Italia, Garante Privacy), in occasione di visite ispettive.	✔	✔	✔				✔							✔	✔	PA - La Società condiziona indebitamente ispettori delle Autorità di Vigilanza al fine di ottenere l'omissione di misure che comportino sanzioni durante visite ispettive. SOC/CP - La Società omette fatti o comunica fatti non veritieri alle Autorità di Vigilanza ovvero a finanzieri e organi di polizia durante attività ispettive. RIC - La Società investe i proventi derivanti dall'evasione fiscale resa possibile dall'occultamento dei libri contabili nell'ambito della propria attività economica (autoriciclaggio). CRI/TSN - Tre o più persone all'interno della Società si associano al fine di commettere un reato rilevante ai sensi del Decreto. TRIB - La Società occulta libri contabili in occasioni di ispezioni dell'Amministrazione tributaria al fine di non consentire la ricostruzione dei redditi o del volume di affari.

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, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24);
- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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.

In particolare, è fatto espresso divieto di:

- 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, etc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;
- procurare indebitamente qualsiasi altro tipo di profitto (licenze, autorizzazioni, sgravi di oneri, anche previdenziali, etc.) con mezzi che costituiscano artifici o raggiri (per esempio invio di documentazione non veritiera);
- influenzare in alcun modo le decisioni di rappresentanti della Pubblica Amministrazione in maniera impropria e/o illecita (come, a titolo di esempio, sollecitare e/o accettare e/o corrispondere e/o offrire ai medesimi, direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per sé o per la Società).

Atti di cortesia commerciale (come, a titolo di esempio, omaggi o forme di ospitalità) sono consentiti solo se non eccedono le normali pratiche commerciali e/o di cortesia e se, in ogni caso, sono tali da non compromettere l'imparzialità e l'indipendenza di giudizio del rappresentante della Pubblica Amministrazione;

- 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.

Inoltre, nel corso della trattativa d'affari o rapporto commerciale sia con la Pubblica Amministrazione che con clienti e fornitori, occorre applicare criteri generali di correttezza, trasparenza e integrità. In particolare, non devono essere esaminate o proposte o promesse opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione o clienti/ fornitori a titolo personale.

Altresì la Società vieta di:

- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva);

quando l'intenzione sia:

- indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di natura pubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
- influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;
- influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio.

Non solo, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

Infine, TeamSystem, al fine di garantire che il processo di selezione, assunzione e gestione del personale rispetti i principi di professionalità, trasparenza e correttezza, secondo quanto previsto dalle Leggi e dai regolamenti applicabili, assicura che tutte le attività siano in conformità alle procedure aziendali e nel rispetto dei principi enunciati nel Codice Anticorruzione.

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:

- è fatto divieto di assumere lavoratori stranieri privi di permesso di soggiorno;
- è fatto divieto di assumere lavoratori il cui permesso sia scaduto – e per il quale non sia richiesto il rinnovo – revocato o annullato;
- è fatto divieto di 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;
- prima di nominare qualunque nuovo membro nel Consiglio di Amministrazione o di assumere, trasferire o promuovere, qualunque nuovo dipendente che è probabile abbia un contatto rilevante con un Pubblico Ufficiale, in relazione alla propria attività lavorativa, che sovrintende dipendenti o partner che è probabile abbiano un tale contatto, o che sarà coinvolto nell'ambito di controlli o altre attività disciplinate dalle Leggi Anticorruzione, TeamSystem deve

informarsi sulle rilevanti esperienze personali del soggetto per quanto consentito dalla legge applicabile, nel rispetto delle disposizioni anticorruzione sulla selezione e assunzione contenute negli strumenti normativi di riferimento adottati dalla Società;

- le procedure interne sulla ricerca, selezione ed assunzione del personale devono prevedere il rispetto di criteri oggettivi e l'effettuazione di controlli sulle referenze e includere nelle richieste d'impiego delle domande adeguate, nei limiti di quanto consentito dalla legge vigente, riguardanti: (a) ogni eventuale precedente penale o imputazione del soggetto; (b) ogni eventuale sanzione civile o amministrativa o indagine in corso che si riferiscono ad attività non etiche o illegali del soggetto, in coerenza con e per quanto consentito dalle leggi applicabili e (c) ogni relazione personale con Pubblici Ufficiali, partner, consulenti, fornitori;
- le assunzioni devono essere precedute da una reale esigenza comprovata dalle autorizzazioni previste dalla normativa interna. L'iter di selezione deve prevedere più passaggi di valutazione da parte di soggettidifferenti;
- la lettera di impegno all'assunzione e il relativo contratto di assunzione devono essere firmate dal soggettoa 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 Aree/ 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;
- deve essere preventivamente richiesto al candidato di dichiarare eventuali rapporti di parentela entro il secondo grado con esponenti della Pubblica Amministrazione e, in caso positivo, deve essere valutata l'eventuale sussistenza di ipotesi di conflitto di interessi;
- 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;
- deve essere effettuato nel continuo il monitoraggio circa la validità dei permessi di soggiorno dei dipendentinon residenti in EU;
- deve valutata 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;
- devono essere svolti un numero variabile di step selettivi (minimo due colloqui) in funzione della posizionericoperta e dell'area di appartenenza;
- i feedback degli incontri dei candidati devono essere tracciabili;
- al candidato deve essere richiesto di dichiarare eventuali conflitti di interesse;
- deve essere verificato che al neo assunto siano stati consegnati i documenti previsti dalla normativa (conparticolare riguardo alla normativa in materia di tutela dei rapporti di lavoro, salute, igiene e sicurezza suiluoghi di lavoro, ambiente, protezione dei dati personali e di responsabilità amministrativa degli enti) e dairegolamenti aziendali interni (tra cui il Codice Etico, il Codice di Condotta Anticorruzione, il Modello Organizzativo, le procedure del sistema di gestione della sicurezza delle informazioni, etc.);
- deve essere previsto che, qualora ci si avvalga di società esterne per il processo di selezione (ad esempio,società di head hunting), il rapporto con le stesse sia formalizzato in appositi contratti, che prevedono l'accettazione delle clausole 231 e del Codice Etico;
- deve essere garantita la tracciabilità delle fonti di reperimento dei CV;
- il processo di ricerca e selezione del personale: (i) deve essere attivato solo in presenza di effettive necessità; (ii) si svolge secondo criteri di obiettività, imparzialità e rispondenza ad interessi di organico;
(iii) si svolge attraverso un processo decisionale trasparente e tracciabile, supportato da idonee evidenzedocumentali in tutte le sue principali fasi; (iv) è approvato ad un adeguato livello autorizzativo, in conformitàal sistema di deleghe e procure adottato; (v) si svolge nel rispetto del principio di segregation of duties, in modo che nessuno possa gestire in autonomia l'intero processo e che sia necessario il coinvolgimento diuna pluralità di soggetti appartenenti a diverse

funzioni aziendali; (vi) nei limiti di quanto consentito dalle leggi vigenti, prevede l'effettuazione di verifiche preventive in merito al rischio di infiltrazione criminale, nonché di possibili condizionamenti illeciti da parte di esponenti della Pubblica Amministrazione o altri soggetti che possano influenzare il processo di selezione;

- è assolutamente vietato offrire o anche solo promettere opportunità di impiego a: rappresentanti della Pubblica Amministrazione, italiana o straniera; persone legate da rapporti personali o familiari; candidati segnalati dai soggetti di cui ai punti precedenti; al fine di influenzare l'indipendenza di giudizio dei rappresentanti della Pubblica Amministrazione o di indurli ad assicurare un qualsiasi vantaggio per l'azienda;
- è fatto divieto di promettere o offrire opportunità di impiego a soggetti privati (ad esempio personale di clienti, fornitori, partner commerciali, etc.), che siano finalizzati ad acquisire vantaggi o trattamenti di favore in modo improprio.

b) Gestione dei benefit aziendali.

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

- devono essere definiti i criteri e le modalità per l'assegnazione dei benefit aziendali;
- deve essere istituito e mantenuto un inventario aggiornato dei beni attribuiti agli assegnatari;
- devono essere definiti i criteri e le modalità per la restituzione dei beni in caso di dimissioni o licenziamento o comunque di interruzione del rapporto di lavoro con la Società;
- i premi devono risultare riconosciuti unicamente nell'ambito del budget approvato e previa autorizzazione degli organi competenti;
- la società deve riconoscere ai dipendenti benefits di varia natura in relazione al ruolo ricoperto (ad esempio, autovettura, tablet, etc.) e ne deve definire l'iter approvativo;
- tutte le variazioni concernenti le mansioni, le condizioni contrattuali di assunzione, l'inquadramento, il livello retributivo, i benefits, etc., devono essere formalizzate ed approvate dal responsabile e dai soggetti individuati come competenti.

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:

- devono essere formalmente stabiliti ed efficacemente svolti controlli periodici sul calcolo e sul pagamento delle remunerazioni variabili;
- eventuali sistemi premianti ai dipendenti e collaboratori devono rispondere ad obiettivi realistici e coerenticon le mansioni, l'attività svolta e le responsabilità affidate;
- tutte le variazioni concernenti le mansioni, le condizioni contrattuali di assunzione, l'inquadramento, il livello retributivo, i benefits, etc., devono essere formalizzate ed approvate dal responsabile dai soggetti individuati come competenti;
- i passaggi di ruolo o di mansione e l'eventuale variazione di livello retributivo devono essere adeguatamente autorizzati ed avvenire secondo criteri obiettivi e documentati;
- il sistema premiante deve rispondere ad obiettivi realistici e coerenti con le mansioni, l'attività svolta e le responsabilità affidate;
- le componenti variabili di retribuzione devono essere liquidate solo a fronte di effettivo raggiungimento deirisultati fissati come obiettivo del sistema premiante, secondo un processo tracciabile e documentato;
- nella definizione degli obiettivi le Aree interessate devono avere cura di evitare target di performance palesemente immotivati ed inarrivabili, che potrebbero costituire un velato incentivo al compimento di alcune delle fattispecie di illecito previste dal Modello Organizzativo;
- l'attribuzione degli emolumenti variabili è approvata congiuntamente dalla Area/ Funzione di riferimento e dai soggetti individuati come competenti;
- eventuali premi di risultato potranno essere riconosciuti unicamente nell'ambito del budget approvato e previa autorizzazione congiunta dei soggetti individuati come competenti e della Area/ Funzione di riferimento.

Area di rischio: Selezione, gestione ed assunzione del personale.

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione delle attività di selezione, assunzione e gestione del personale.	✓	✓					✓		✓			✓				PA - La Società strumentalizza ad interesse o vantaggio proprio, l'assunzione di risorselegate o gradite ad esponenti o enti della Pubblica Amministrazione. 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 propriopersonale benefit aziendali affinché attraverso l'utilizzo con terzi possa ottenere in cambio un beneficio per il business.

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 all'attività sensibile:

- Gestione del contenzioso giudiziale e stragiudiziale e dei rapporti: (i) 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; (ii) con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale; (iii) con la controparte per accordi stragiudiziali.

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, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25);
- reati societari (art. 25-ter);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 - decies);
- delitti di criminalità organizzata (art. 24-ter);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies);
- reati tributari (art. 25-quinquiesdecies);
- reati transnazionali (art. 10, L. 146/2006).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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.

In particolare, è fatto espresso divieto di:

- 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, etc. e richieste di

finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;

- procurare indebitamente qualsiasi altro tipo di profitto (licenze, autorizzazioni, sgravi di oneri, anche previdenziali, etc.) con mezzi che costituiscano artifici o raggiri (per esempio invio di documentazione non veritiera);
- influenzare in alcun modo le decisioni di rappresentanti della Pubblica Amministrazione in maniera impropria e/o illecita (come, a titolo di esempio, sollecitare e/o accettare e/o corrispondere e/o offrire ai medesimi, direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per sé o per la Società). Atti di cortesia commerciale (come, a titolo di esempio, omaggi o forme di ospitalità) sono consentiti solo se non eccedono le normali pratiche commerciali e/o di cortesia e se, in ogni caso, sono tali da non compromettere l'imparzialità e l'indipendenza di giudizio del rappresentante della Pubblica Amministrazione;
- 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;
- in occasione di un procedimento giudiziario e/o di un'indagine/ispezione da parte delle Autorità pubbliche:
  - distruggere/ alterare registrazioni, verbali, scritture contabili e qualsiasi altro tipo di documento,
  - mentire o fare/ intimare a fare dichiarazioni false alle autorità competenti;

  qualsiasi tentativo di estorsione o di concussione da parte di un pubblico ufficiale devono essere segnalati al proprio Responsabile.

Inoltre, la Società vieta di:

- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva); quando

l'intenzione sia:

- indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di natura pubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
- influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;
- influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

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; con la controparte per accordi stragiudiziali.**

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, con la controparte per accordi stragiudiziali, i protocolli prevedono che:

- è fatto l'assoluto divieto di:
  - porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare indebitamente una delle parti in causa del contenzioso;
  - elargire o anche solo promettere a pubblici ufficiali e incaricati di pubblico servizio (quali magistrati, arbitri, funzionari di cancelleria, periti, testimoni, ufficiali giudiziari, etc.), ovvero a persone comunque suggerite da tali soggetti, denaro o qualsiasi altra utilità (ad esempio, la promessa di assunzione di un familiare del pubblico funzionario);
  - adottare comportamenti contrari alla legge e ai principi aziendali per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della controparte (anche tramite soggetti terzi quali professionisti e legali esterni);
  - usare violenza o minaccia, o, in alternativa, l'offerta di denaro o altra utilità, per indurre un collega o qualsiasi altra persona a non rendere dichiarazioni all'Autorità giudiziaria, a rendere dichiarazioni non veritiere, non complete o non corrette all'Autorità giudiziaria, o comunque per indurla ad alterare in qualsiasi modo il contenuto delle proprie dichiarazioni.
  - 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;
  - 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;
  - fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di cui alla presente Parte Speciale;
  - 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;
  - 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;
  - selezionare i soggetti autorizzati ad interloquire con i dipendenti coinvolti in procedimenti penali, e gli eventuali colloqui intercorsi verbalizzati;
  - concludere transazioni fittizie al sol fine di registrare o far registrare a terzi elementi passivi fittizi;
- l'ingaggio di legali esterni è svolto solo da personale autorizzato, in coerenza con il sistema di deleghe e procure adottato;
- i compensi dei legali esterni devono essere corrisposti in misura congrua rispetto alle prestazioni rese in favore della Società, in conformità al contratto di mandato o alla lettera di incarico sottoscritto e sono sostanzialmente congrui rispetto alle condizioni o prassi esistenti sul mercato o alle tariffe professionali vigenti;
- deve essere assicurata la predisposizione di uno scadenzario che permetta di controllare l'intera attività esecutiva, con particolare riferimento al rispetto dei termini processuali previsti;
- deve essere assicurata la corretta archiviazione della documentazione relativa al contenzioso allo scopo di garantire la tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate;
- gli accordi transattivi devono essere conclusi in base a valutazioni tracciabili e autorizzati da soggetti in possesso di adeguati poteri di rappresentanza;

- i rapporti con i legali devono essere mantenuti dall'Ufficio Legale o da soggetti autorizzati;
- qualora la Società si avvalga di legali/ professionisti esterni per la gestione del contenzioso, il relativo contratto/ lettera di incarico deve contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- l'incarico a professionisti esterni deve essere conferito per iscritto, con indicazione del compenso pattuito o del metodo di determinazione degli onorari e delle spese che saranno oggetto di fatturazione oltre alla chiara e puntuale descrizione del contenuto della prestazione. Gli onorari devono essere sostanzialmente congrui rispetto alle condizioni o prassi esistenti sul mercato o alle tariffe professionali vigenti, avuto riguardo alla complessità e alla natura dell'attività prestata;
- il processo di approvazione del pagamento degli onorari e delle spese di assistenza deve essere eseguito nel rispetto dei livelli autorizzativi;
- per giungere ad una transazione, devono ricorrere i requisiti di sussistenza dei presupposti giuridici, nonché la convenienza economica per la Società;
- l'articolazione del processo deve garantire la segregazione funzionale tra i coloro che agiscono nell'ambito del processo di gestione del contenzioso.

Area di rischio: Gestione dei contenziosi giudiziali e stragiudiziali.

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
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 al fine di ottenere un accordo transattivo vantaggioso. RIC - La Società investe i proventi derivanti dall'evasione fiscale, perpetrata tramite la conclusione di accordi transattivi fittizi, nell'ambito della propria attività economica (autoriciclaggio). 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. CRI/TSN - Tre o più persone all'interno della Società si associano al fine di commettere un reato rilevante ai sensi del Decreto. TRIB - La Società conclude un accordo transattivo fittizio con un terzo al fine di creare passività fittizie da indicare nelle dichiarazioni pertinenti e evadere le imposte sui redditi

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: (i) rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (ad esempio, gestione e registrazione contabile della fatturazione attiva); (ii) verifica dati provenienti dai sistemi informativi alimentanti; (iii) accertamento dei costi e dei ricavi di competenza del periodo; (iv) definizione delle postevalutative; (v) raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato; (vi) tenuta e custodia della documentazione obbligatoria e delle scritture contabili;
- Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività: (i) registrazione delle fatture passive/ note di credito e debito; (ii) autorizzazione e invio dei pagamenti; (iii) inserimento/modifica delle coordinate bancarie del fornitore; (iv) alienazione e vendita di asset;
- Gestione dei rapporti con gli istituti finanziari;
- Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo;
- Rimborsi spese, anticipi e spese di rappresentanza.

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:

- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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 tributari (art. 25-quinquiesdecies);
- reati transnazionali (art. 10, L. 146/2006).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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.

In particolare, è fatto espresso divieto di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;
- 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;
- 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;
- 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;
- girare per l'incasso assegni bancari e postali emessi all'ordine del traente a soggetti diversi da banche o Poste Italiane S.p.A.;
- promettere o effettuate erogazioni in denaro a favore di rappresentati della Pubblica Amministrazione, per finalità diverse da quelle istituzionali e di servizio;
- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva);

  quando l'intenzione sia di:

  - indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di natura pubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
  - influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;
  - influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio

Inoltre, la Società richiede che i rapporti con le terze parti – fornitori, clienti, consulenti, e altre persone fisiche, persone giuridiche (anche appartenenti allo stesso Gruppo TeamSystem) ed enti di fatto – intrattenuti durante lo svolgimento delle attività di business, siano improntati a criteri di massima correttezza, trasparenza e tracciabilità delle fonti informative, nonché nel rispetto delle Leggi Anticorruzione e di tutte le altre leggi applicabili.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori;

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 (ad esempio, gestione e registrazione contabile della fatturazione attiva);**
- **verifica dati provenienti dai sistemi informativi alimentanti;**
- **accertamento dei costi e dei ricavi di competenza del periodo;**
- **definizione delle poste valutative;**
- **raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di bilancio civilistico e consolidato;**
- **tenuta e custodia della documentazione obbligatoria e delle scritture contabili.**

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 (ad esempio, gestione e registrazione contabile della fatturazione attiva); verifica dati provenienti dai sistemi informativi alimentanti; accertamento dei costi e dei ricavi di competenza del periodo; definizione delle poste valutative; raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato; tenuta e custodia della documentazione obbligatoria e delle scritture contabili, i protocolliprevedono che:

- le registrazioni contabili possono essere effettuate esclusivamente da soggetti abilitati nell'uso del sistemainformatico 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;
- tutte le informazioni strumentali al processo valutativo o di stima delle voci di bilancio devono essere archiviate sotto la responsabilità delle Aree/ Funzioni aziendali che producono/ricevono tali informazioni;
- 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;
- ogni modifica ai dati contabili deve essere effettuata dalla sola Area/ Funzione che li ha generati, garantendo la tracciabilità dell'operazione di modifica e previa formale autorizzazione del Responsabile diArea/ Funzione;
- devono essere 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 daimpedire successive modifiche e agevolare futuri controlli;
- la Società è tenuta a custodire in modo corretto ed ordinato le scritture contabili e gli altri documenti di cuisia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscanoeventuali atti di distruzione e/o occultamento;
- è fatto divieto di occultare o distruggere in tutto o in parte e scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affaridella Società;
- l'Area Amministrazione, Finanza e Controllo, in sede di determinazione del fondo imposte, deve effettuarecontrolli circa l'inerenza fiscale dei costi contabilizzati analizzando i conti ritenuti più significativi (o per importo o per la natura dei costi imputati);
- la Società ha definito criteri predeterminati ed oggettivi da utilizzare per la valutazione delle poste valutative;

- l'Area Amministrazione, Finanza e Controllo, in sede di determinazione delle poste valutative, deve verificare la corretta applicazione dei criteri utilizzati per le poste valutative. Eventuali deroghe a tali criterisono autorizzate da posizione gerarchiche adeguate;
- tutti i documenti ufficiali volti ad illustrare la situazione gestionale delle società del Gruppo devono essere redatti con la massima cura al fine di garantirne l'accuratezza e veridicità. Devono, inoltre, essere redatti in conformità delle leggi e normative vigenti;
- nella redazione dei predetti documenti, il personale di TeamSystem deve prestare la dovuta attenzione e mantenere quei comportamenti improntati a principi di correttezza, onestà e integrità che devono informarelo svolgimento delle attività professionali di propria competenza. In ogni caso non sarà giustificata né giustificabile la tenuta / redazione di documentazione deliberatamente falsa o artefatta in modo da alterare significativamente la rappresentazione veritiera della situazione di TeamSystem;
- in ogni caso non sarà giustificata né giustificabile la tenuta / redazione di documentazione deliberatamentefalsa o artefatta in modo da alterare significativamente la rappresentazione veritiera della situazione di TeamSystem;
- ogni operazione, azione e transazione della società deve essere adeguatamente registrata e documentatain modo da consentire la verifica dei processi di decisione, autorizzazione e svolgimento;
- ogni atto od operazione svolta dal personale dovrà essere supportata da documentazione adeguata, chiara e completa e dovrà essere conservata in modo da consentire in ogni momento il controllo sulle motivazioni, le caratteristiche dell'operazione e l'individuazione dei soggetti che hanno eseguito l'operazione, che hanno concesso le autorizzazioni e che hanno effettuato le verifiche;
- tutte le Aree/ Funzioni aziendali sono tenute a prestare la massima collaborazione al fine di garantire registrazioni contabili corrette e tempestive. Le registrazioni contabili fondate su valutazioni economico- patrimoniali devono rispettare i criteri di ragionevolezza e prudenza;
- per ogni registrazione contabile deve essere conservata agli atti un'adeguata documentazione. Tale documentazione deve consentire di individuare il motivo dell'operazione che ha generato la rilevazione e la relativa autorizzazione. La documentazione di supporto deve essere archiviata e facilmente consultabile;
- chiunque venga a conoscenza di possibili omissioni, falsificazioni o irregolarità nella tenuta della contabilità deve darne immediata comunicazione al proprio superiore;
- nello svolgimento delle attività di verifica e controllo da parte del Collegio Sindacale, dei Revisori e dei Soci è necessario agire con trasparenza e prestare la massima collaborazione;
- le leggi applicabili, le leggi e i regolamenti sull'informativa finanziaria e le leggi fiscali richiedono che TeamSystem mantenga scritture contabili dettagliate e complete di ogni operazione di business. Le scritture della Società devono conformarsi ai principi contabili applicabili e devono riflettere in modo completo e trasparente i fatti alla base di ogni operazione;
- tutti i costi e gli addebiti, le entrate e gli incassi, gli introiti, i pagamenti e gli impegni di spesa devono essereinseriti tempestivamente tra le informazioni finanziarie, in maniera completa e accurata ed avere adeguatidocumenti di supporto, emessi in conformità con tutte le leggi applicabili e con le relative disposizioni del sistema di controllo interno. Tutte le registrazioni nelle scritture contabili e la relativa documentazione informativa devono essere a disposizione del revisore esterno per le attività di controllo;
- è policy di TeamSystem che tutti i pagamenti e le operazioni della Società debbano essere registrate accuratamente nei relativi libri e registri della società interessata, di modo che i libri, i registri e la contabilità di TeamSystem riflettano dettagliatamente e correttamente le operazioni e le disposizioni dei beni con ragionevole dettaglio. Tale principio si applica a tutte le operazioni e le spese, siano esse significative o meno sotto il profilo contabile. Inoltre, come previsto dalle procedure interne, sono specificatamente definitii criteri contabili e i conti di bilancio da adottare per la registrazione delle operazioni di business; tutte le operazioni sono registrate nei libri contabili in forma veritiera e corretta;
- la Società ha definito un iter operativo e un calendario per quanto riguarda gli adempimenti ricorrenti (ad esempio, registrazione dei flussi contabili);
- la Società ha definito un iter operativo e dei ruoli e responsabilità relativi alla gestione della contabilità generale;
- la Società ha definito un iter operativo per quanto riguarda la predisposizione del bilancio d'esercizio;

- ogni fatto amministrativo e la relativa registrazione in contabilità generale deve essere verificabile mediante la corrispondente documentazione di supporto e deve avvenire conformemente ai relativi flussi autorizzativi sottostanti;
- l' Area Amministrazione, Finanza e Controllo predispone il calendario delle attività di chiusura che devono essere espletate per la predisposizione del Progetto di Bilancio d'esercizio;
- una volta effettuate le eventuali modifiche/integrazioni/correzioni contabili, si provvede a rielaborare il Bilancio di Verifica, del quale l' Area Amministrazione, Finanza e Controllo archivia l'ultima versione

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

- **registrazione delle fatture passive/ note di credito e debito;**
- **autorizzazione e invio dei pagamenti;**
- **inserimento/modifica delle coordinate bancarie del fornitore;**
- **alienazione e vendita di asset.**

Per l'attività sensibile Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività registrazione delle fatture passive/ note di credito e debito; autorizzazione e invio dei pagamenti; inserimento/modifica delle coordinate bancarie del fornitore; alienazione e vendita di asset, i protocolli prevedono che:

- deve essere assicurata la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi;
- 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 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;
- devono essere vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minimi di spesa espressamente autorizzate dalla funzione amministrazione, ed in particolare per le operazioni di piccola cassa;
- devono essere 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;
- tutte le fatture ricevute, a fronte di impegni di spesa, devono essere formalizzate attraverso un contratto o un ordine di acquisto;
- è necessario accertare la corrispondenza tra il documento di trasporto (DDT) e la quantità di beni ricevuti;
- è necessario accertare la corrispondenza tra l'ordine di acquisto, il bene/servizio ricevuto e la relativa fattura;

- 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 memorandum redatto e firmato dalla Area/ Funzione richiedente che specifichi le motivazioni della mancanza della documentazione stessa;
- è fatto divieto di effettuare prestazioni e/o riconoscere compensi in favore di consulenti, partner, fornitori oaltrisoggetti terzi che non trovino adeguata giustificazione nel rapporto contrattuale costituito con gli stessi;
- è fatto divieto di effettuare qualunque tipo di pagamento nell'interesse della Società in mancanza di adeguata documentazione di supporto;
- 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 previsto che i pagamenti siano effettuati sulla base dell'effettiva esistenza di documentazionecontabile di riferimento;
- deve essere previsto che i pagamenti possano essere effettuati solo a soggetti preventivamente censiti inanagrafica;
- deve essere prevista la verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ ordinanti dei pagamenti e controparti effettivamente coinvolte nella transazione;
- devono essere previsti controlli sulla classificazione della fornitura (spesabile / capitalizzabile);
- devono essere previsti controlli sul match fattura–ordine ed eventuali autorizzazioni sui mismatch;
- deve essere stabilito che solo le fatture autorizzate vanno in payment list e che siano effettuati controlli sueventuali eccezioni (ad esempio, pagamenti anticipati);
- devono essere predisposti blocchi informatici sulle duplicazioni degli ordini di acquisto e sui campi chiave dell'anagrafica fornitori;
- devono essere previsti controlli automatici sul numero della partita IVA e sulle fatture duplicate;
- deve essere effettuata attività di riconciliazione, sia dei conti intercompany, sia dei conti intrattenuti conistituti di credito;
- deve essere effettuata la riconciliazione di tutti i saldi di conto corrente con le relative schede contabili,sulla base degli estratti conto bancari;
- è fatto divieto di emettere fatture o rilasciare documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- deve essere garantita nell'ambito dell'emissione delle fatture attive: (i) la corretta indicazione del cliente, del numero e data fattura; (ii) che sia riportata la corretta descrizione dell'IVA applicabile; (iii) che i dati inerenti alle fatture attive siano accuratamente trasferiti nel libro giornale, nel partitario clienti e nel registroIVA vendite; (iv) la correttezza del conteggio inerente all'applicazione della ritenuta d'acconto;
- devono essere previsti controlli di sistema che non consentono l'emissione di fatture attive: (i) in assenza del completamento del work-flow; (ii) in assenza della documentazione attestante l'avvenuta messa a disposizione/erogazione del servizio; (iii) in assenza di corrispondenza di quanto fatturare rispetto a quantoprevisto contrattualmente; (iv) la duplice registrazione di documenti contabili emessi dal medesimo cliente nello stesso esercizio;
- le richieste di cessione/ dismissione di asset devono essere formalmente emesse da parte del responsabile di centro di costo. A seconda della tipologia/importo di asset da dismettere/vendere sono definite regole formalizzate che prevedono il coinvolgimento degli opportuni livelli di management;
- nei casi di vendita di cespiti, queste devono essere oggetto di regolare fatturazione in linea con gli accordicontrattuali stipulati;
- i driver utilizzati per la determinazione del prezzo di vendita degli asset devono essere definiti in maniera formalizzata e trasparente anche al fine di garantire che la valorizzazione sia in linea con la quotazione dimercato del bene;
- ogni operazione, azione e transazione della società deve essere adeguatamente registrata e documentatain modo da consentire la verifica dei processi di decisione, autorizzazione e svolgimento;
- ogni atto od operazione svolta dal personale dovrà essere supportata da documentazione adeguata, chiara e completa e dovrà essere conservata in modo da consentire in ogni momento il controllo sulle motivazioni, le caratteristiche

dell'operazione e l'individuazione dei soggetti che hanno eseguito l'operazione, che hanno concesso le autorizzazioni e che hanno effettuato le verifiche;

- le leggi applicabili, le leggi e i regolamenti sull'informativa finanziaria e le leggi fiscali richiedono che TeamSystem mantenga scritture contabili dettagliate e complete di ogni operazione di business. Le scritture della Società devono conformarsi ai principi contabili applicabili e devono riflettere in modo completo e trasparente i fatti alla base di ogni operazione;
- tutti i costi e gli addebiti, le entrate e gli incassi, gli introiti, i pagamenti e gli impegni di spesa devono essereinseriti tempestivamente tra le informazioni finanziarie, in maniera completa e accurata ed avere adeguatidocumenti di supporto, emessi in conformità con tutte le leggi applicabili e con le relative disposizioni del sistema di controllo interno. Tutte le registrazioni nelle scritture contabili e la relativa documentazione informativa devono essere a disposizione del revisore esterno per le attività di controllo;
- è policy di TeamSystem che tutti i pagamenti e le operazioni della Società debbano essere registrate accuratamente nei relativi libri e registri della società interessata, di modo che i libri, i registri e la contabilità di TeamSystem riflettano dettagliatamente e correttamente le operazioni e le disposizioni dei beni con ragionevole dettaglio. Tale principio si applica a tutte le operazioni e le spese, siano esse significative o meno sotto il profilo contabile. Inoltre, come previsto dalle procedure interne, sono specificatamente definitii criteri contabili e i conti di bilancio da adottare per la registrazione delle operazioni di business; tutte le operazioni sono registrate nei libri contabili in forma veritiera e corretta;
- la Società ha definito un iter operativo e un calendario per quanto riguarda gli adempimenti ricorrenti (ad esempio, registrazione dei flussi contabili);
- la Società ha definito un iter operativo e dei ruoli e responsabilità relativi alla gestione della contabilità generale;
- la Società ha definito un iter operativo per quanto riguarda la predisposizione del bilancio d'esercizio;
- l' Area Amministrazione, Finanza e Controllo predispone il calendario delle attività di chiusura che devono essere espletate per la predisposizione del Progetto di Bilancio d'esercizio;
- una volta effettuate le eventuali modifiche/ integrazioni/correzioni contabili, si provvede a rielaborare ilBilancio di Verifica del quale l' Area Amministrazione, Finanza e Controllo archivia l'ultima versione.

b) 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 necessario garantire 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;
- deve essere assicurata la verificabilità e documentabilità delle operazioni;
- 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;
- anche la scelta dei partner deve ricadere su operatori che rispondono a criteri di eticità, affidabilità, buona reputazione, credibilità nel mercato di riferimento e serietà professionale.

c) 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 che:

- è necessario definire i criteri di determinazione e gestione dei prezzi di trasferimento, con indicazione del perimetro di applicazione degli stessi, ove sia necessario (ad esempio, ambito transfer price);
- è necessario definire chiaramente la funzione responsabile della definizione delle caratteristiche del contratto intercompany;
- è necessario definire le attività di monitoraggio dei rapporti infragruppo;
- è necessario effettuare un'attività di riconciliazione dei conti intercompany;
- tutte le fatture ricevute, a fronte di impegni di spesa, devono essere formalizzate attraverso un contratto o un ordine di acquisto;
- deve essere accertata la corrispondenza tra il documento di trasporto (DDT) e la quantità di merce ricevuta;
- deve essere accertata la corrispondenza tra l'ordine di acquisto, i beni/servizi ricevuti e la relativa fattura;
- le movimentazioni di cash pooling devono essere tracciabili e monitorate tramite sistema di remote banking e sistema gestionale Gamma Enterprise;
- le movimentazioni di cash pooling devono essere verificate dall'Area Amministrazione, Finanza e Controllo: (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 controllo di gestione, interrogando lo specifico conto di contabilità generale acceso al rapporto di cash pooling;
- deve essere definito il contratto che disciplina le modalità e i principi con i quali sono gestiti i rapporti tra la Società e le Società controllate, collegate e controllanti;
- devono essere descritte all'interno del contratto intercompany le attività svolte per conto della controparte;
- ciascuna operazione infragruppo deve avvenire sulla base di documentazione autorizzata da soggetti dotati di idonei poteri;
- l'Area competente di prendere in carico i contratti di servizio infragruppo sottoscritti dalla Società e le altre società del gruppo, deve verificare, con il supporto delle competenti unità, che il documento sia redatto secondo lo standard predisposto, che contenga l'elenco dei beni/servizi resi, i relativi prezzi e che sia firmato da soggetti dotati di adeguati poteri di firma, lasciando evidenza del controllo eseguito;
- deve essere verificato, con riferimento agli acquisti intercompany, che la fornitura di beni o di servizi sia avvenuta a condizioni di mercato.

d) Rimborsi spese, anticipi e spese di rappresentanza.

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

- non devono essere ammessi anticipi o rimborsi delle spese sostenute direttamente dai soggetti esterni, in particolare da rappresentanti della Pubblica Amministrazione che beneficiano di ospitalità;
- 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, etc.) 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 vantaggiimpropri;
- l'Area Amministrazione, Finanza e Controllo 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;
- deve essere assicurata la tracciabilità delle note spese e dei relativi giustificativi;
- tutte le fatture ricevute devono essere, a fronte di impegni di spesa, formalizzate attraverso un contratto oun ordine di acquisto;
- deve essere accertata la corrispondenza tra il documento di trasporto (DDT) e la quantità di beni ricevuta;
- deve essere accertata la corrispondenza tra l'ordine di acquisto, i beni/ servizi ricevuti e la relativa fattura;
- nel corso della trattativa d'affari o rapporto commerciale sia con la Pubblica Amministrazione che con clienti e fornitori, occorre applicare criteri generali di correttezza, trasparenza e integrità. In particolare, non devono essere:
  - esaminate o proposte o promesse opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione o clienti/ fornitori a titolo personale;
  - offerti in alcun modo omaggi, dazioni, benefici anche indiretti, beni, servizi e prestazioni o favori non dovuti o che travalichino gli ordinari rapporti di cortesia;
  - sollecitate o ottenute informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti, nonché arrecare benefici diretti o indiretti rilevanti per sé o per la Società;
  - intraprese azioni volte a influenzare impropriamente le decisioni della controparte.
- qualsiasi forma di ospitalità o di rappresentanza concessa in un periodo immediatamente antecedente o successivo, ad esempio, ad una procedura di gara, è da considerare inappropriata in quanto potrebbe essere interpretata come un atto corruttivo avente la finalità di chiudere l'accordo ottenendo un indebito vantaggio;
- tutte le spese di rappresentanza devono essere registrate in maniera accurata e trasparente nei libri contabili della Società con sufficiente dettaglio e devono essere supportate da adeguata documentazionegiustificativa al fine di individuare il nome dei beneficiari, nonché la finalità del pagamento.

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

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione della contabilità generale, con particolare riferimento alle attività di: - rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (ad esempio, gestione e registrazione contabile della fatturazione attiva); - verifica dati provenienti dai sistemi informativi alimentanti; - accertamento dei costi e dei ricavi di competenza del periodo; - definizione delle poste valutative; - raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato - tenuta e custodia della documentazione obbligatoria e delle scritture contabili		✔	✔				✔							✔	✔	SOC/CP - La Società inserisce in bilancio o in altri documenti contabili informazioni false al fine di ingannare soci e pubblico. RIC - La Società investe i proventi derivanti dall'evasione fiscale, resa possibile dall'occultamento dei libri contabili, nell'ambito della propria attività economica (autoriciclaggio). CRI/TSN - Tre o più persone all'interno della Società si associano al fine di commettere un reato rilevante ai sensi del Decreto. TRIB - Distruzione e/o occultamento di documentazione contabile e obbligatoria per occultare le prove di una non corretta tenuta delle scritture contabili ai fini di evadere le imposte sui redditi o sul valore aggiunto

Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività: - registrazione delle fatture passive/ note di credito e debito - autorizzazione e invio dei pagamenti; - inserimento/modifica delle coordinate bancarie del fornitore; - alienazione e vendita di asset.	✔	✔	✔				✔						✔	✔	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. // La Società investe i proventi derivanti dall'evasione fiscale, perpetrata tramite la registrazione di elementi passivi fittizi, nell'ambito della propria attività economica (autoriciclaggio). 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. TRIB - La Società contabilizza fatture per operazioni inesistenti al fine di registrare elementi passivi fittizi o si avvale di documenti falsi o di altri mezzi fraudolenti che comportino l'indicazione di elementi attivi per un ammontare inferiore a quello effettivo o di elementi passivi fittizi o crediti e ritenute fittizi al fine di evadere le imposte sui redditi o sul valore aggiunto.
Gestione dei rapporti con gli istituti finanziari.		✔													SOC/CP - Stipulare un accordo favorevole alla Società ma svantaggioso alla Controparte in cambio di denaro o altra utilità.
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. TRIB - La Società contabilizza fatture per operazioni inesistenti con controparti intercompany o emette fatture per operazioni inesistenti nei confronti di controparti intercompany.
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.

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 (ad esempio, M&A).
- Gestione delle operazioni sul capitale sociale (ad 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);
- 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 tributari (art. 25-quinquiedecies);
- reati transnazionali (art. 10, L. 146/2006).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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.

Infatti, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

Protocolli specifici di prevenzione

a) Gestione delle operazioni straordinarie (ad esempio, M&A).

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

- tutte le operazioni straordinarie devono sottoposte e approvate dal Consiglio di Amministrazione della Società;

- devono essere 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;
- in conformità e nei limiti di quanto consentito dalla normativa in materia di protezione dei dati personali, devono essere preventivamente svolti accertamenti per verificare la sussistenza in capo alla controparte dell'operazione di condanne definitive o di procedimenti penali (ad esempio, carichi pendenti, precedenti penali) dai quali potrebbero derivare condanne ai sensi e agli effetti del Decreto;
- deve essere 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;
- deve essere verificata preliminarmente la completezza, inerenza e correttezza della documentazione di supporto dell'operazione;
- devono essere svolte 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 (due diligence contabile e finanziari, di business, legale e/o fiscale, sulla sicurezza del prodotto e sugli aspetti di protezione dei dati personali);
- devono essere adeguatamente considerati, identificati e mitigati i rischi in materia di sicurezza e protezione dei dati personali degli interessati;
- il processo di autorizzazione e controllo delle operazioni straordinarie deve svolgersi nel rispetto dei seguenti principi: (i) coerenza delle iniziative con le strategie di TeamSystem; (ii) separazione delle responsabilità di autorizzazione, esecuzione e controllo; (iii) delega all'autorizzazione differenziata in base alla rilevanza delle iniziative; (iv) rigore metodologico di valutazione; (v) omogeneità degli scenari e delle analisi dei mercati di riferimento sottostanti le valutazioni;
- la Società, con il supporto di eventuali advisor specialistici, deve avviare le attività di due diligence esterna (in caso di acquisizione), interna (in caso di cessioni) sull'oggetto della compravendita. Il rapporto di due diligence da elaborare deve contenere: nominativi delle persone che hanno condotto le attività di due diligence; esami effettuati e i relativi esiti; deduzioni e raccomandazioni fatte; eventuali modifiche agli accordi da proporre alla controparte;
- una volta conclusa la due diligence e verificata la fattibilità dell'operazione, la Società deve redigere una nota contenente: (i) descrizione dell'operazione; (ii) sintesi dei risultati della valutazione economica; (iii) principali evidenze delle attività di due diligence; (iv) principali evidenze delle attività di due diligence sul partner; (v) proposta di acquisto o di vendita (prezzo e principali condizioni). L'organo deliberante esamina ed eventualmente approva la proposta dell'operazione;
- tutta la documentazione prodotta nell'ambito delle attività di gestione delle operazioni straordinarie comprese eventuali comunicazioni via e-mail, è conservata a cura dei diversi responsabili di Area/Funzione coinvolti nell'operazione e messa a disposizione, su richiesta, del Presidente, del Collegio Sindacale, della Società di Revisione e dell'Organismo di Vigilanza. I documenti prodotti nell'ambito delle attività menzionate devono essere conservati per la durata di 10 (dieci) anni;
- è essenziale inserire nel contratto di acquisizione adeguate disposizioni anticorruzione, nonché, prima della chiusura della transazione, prendere in considerazione altre opzioni disponibili per evitare di subentrare in responsabilità.

I protocolli interni prevedono, altresì, che è severamente vietato:

- diffondere l'informazione rilevante all'interno o all'esterno della Società, se non tramite il canale istituzionalmente previsto;
- 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;
- 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;
- 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;
- diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo;
- raccomandare o indurre soggetti terzi a compiere le azioni di cui ai punti precedenti, sulla base delle medesime informazioni;
- 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.

b) Gestione delle operazioni sul capitale sociale (ad 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;
- tutte le operazioni straordinarie devono essere sottoposte e approvate dal Consiglio d'Amministrazione della Società.
- nel caso in cui TeamSystem e/o il Gruppo decidesse di effettuare un'operazione straordinaria non rientrante nelle operazioni considerate come di M&A, la Direzione Amministrazione Finanza e Controllo procede a nominare un Project Leader;
- 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;
- tutti i Destinatari sono tenuti, nello svolgimento delle proprie mansioni, alla corretta gestione delle informazioni privilegiate nonché alla conoscenza e al rispetto delle procedure aziendali con riferimento al market abuse;
- è fatto espresso divieto di ogni comportamento atto a costituire, o che possa agevolare, insider trading. In ogni caso, le operazioni di acquisto o vendita di strumenti finanziari di TeamSystem o di società esterne a TeamSystem dovranno essere sempre compiute in modo trasparente.

Area di rischio: Gestione delle operazioni straordinarie

	Categorie di reato	

Attività sensibili	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	Esempi di reato
Gestione delle operazioni straordinarie (ad esempio, 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 (autoriciclaggio). CRI / TSN - La Società intrattiene rapporti (ad esempio, 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. TRIB - Al fine di sottrarsi al pagamento di imposte sui redditi, la Società aliena simulatamente partecipazioni societarie al fine di rendere in tutto o in parte inefficaci eventuali procedure di riscossione coattiva.
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), compreso l'accesso ai sistemi informativi contabili;
- Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni, compresol'accesso ai sistemi informativi contabili;
- Gestione della installazione dei software applicativi aziendali interni;
- 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);
- delitti di criminalità organizzata (art. 24-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-quinquiedecies).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, che costituiscono parte integrantedello 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 conformialla 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:

- le risorse informatiche sono di proprietà aziendale: gli utenti sono tenuti a custodirle diligentemente, senzaarrecarvi danno e a restituirle tempestivamente in caso di cessazione del rapporto di lavoro o contrattualecon la Società e in ogni altro caso in cui la Società revochi all'utente l'autorizzazione ad accedere alle risorse informatiche o ritenga necessario provvedere alla sostituzione di tali risorse informatiche;

- è rigorosamente vietato: (I) accedere alle risorse informatiche mediante credenziali di autenticazione o profili di autorizzazione diversi da quelli assegnati; (II) comunicare ad altri la propria password o annotarla vicino ai punti di accesso alle risorse informatiche; (III) lasciare incustodite le risorse informatiche (prestando particolare attenzione ai supporti mobili o rimovibili) o consentirne l'accesso a soggetti non autorizzati; (IV) modificare le configurazioni hardware e software preimpostate sulle risorse informatiche (ad esempio tramite l'installazione di programmi non autorizzati, schede wireless, modem, webcam, software di interfaccia con cellulari etc.), salvo previa autorizzazione esplicita dell'Amministratore di Sistema; (V) utilizzare dispositivi o supporti di memorizzazione (ad esempio, hard disk esterni o chiavi USB) non autorizzati e comunque per ragioni non inerenti all'attività lavorativa. Anche qualora tali operazioni siano consentite, la detenzione dei dati memorizzati dovrà essere limitata al tempo strettamente necessario per l'espletamento delle attività connesse; (VI) cancellare, copiare o rimuovere programmi software senza autorizzazione; (VII) abilitare la password del bios senza autorizzazione; (VIII) effettuare operazioni di download, duplicazione, memorizzazione di files e/o dati non strettamente attinenti all'attività lavorativa; (IX) distruggere, deteriorare, cancellare indebitamente informazioni, dati o programmi software altrui; (X) utilizzare software o hardware o qualsivoglia altro strumento o apparecchiatura atta a intercettare, falsificare, alterare o distruggere il contenuto di documenti informatici, a monitorare o controllare le attività di altri utenti o di terzi, leggerne i file o ad interrompere comunicazioni relative ad un sistema informatico o telematico altrui (quali, ad esempio, virus, worm, trojan, spyware, dialer, keylogger, rootkit, etc.); (XI) alterare e/o modificare indebitamente, mediante l'utilizzo di firma elettronica altrui o in qualsiasi altro modo, documenti informatici; (X) elaborare o trasmettere per via informatica o telematica dati falsi e/o alterati; (XII) introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza; (XIII) 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; (XIV) trasmettere, scaricare o archiviare tramite le risorse informatiche materiale di natura oscena, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica; (XV) utilizzare le risorse informatiche per qualsiasi altra finalità contraria alle norme di legge o al buon costume (compreso l'utilizzo di giochi d'azzardo on-line, etc.);
- l'utilizzo di dispositivi personali è consentita solo previa autorizzazione del proprio responsabile;
- il dipendente e/o il collaboratore deve accettare di rispettare le regole generali finalizzate a garantire la protezione dei dati riservati memorizzati o a cui si accede utilizzando un dispositivo mobile personale utilizzato nell'ambito dell'attività lavorativa, ed in particolare:
- l'accesso alla rete aziendale e alla posta elettronica è consentito solamente agli utenti autorizzati esolamente in base alle credenziali di autenticazione o profili di autorizzazione assegnati;
- è vietato l'utilizzo di caselle di posta elettronica personali per lo svolgimento di attività lavorativa;
- è vietato inviare a soggetti non autorizzati files o dati di proprietà della Società;
- agli utenti è strettamente vietato: (I) partecipare a forum, chat line, guests book o altri strumenti di conversazione o discussione non pertinenti all'attività lavorativa; (II) utilizzare pseudonimi, nickname, o strumenti che consentono di restare anonimi o di alterare la propria identità; (III) inviare file o dati verso internet (upload) per scopi estranei alle proprie mansioni lavorativa; (IV) installare software "peer to peer" o comunque procurarsi in qualsiasi altro modo, trasmettere o detenere materiale in violazione del diritto di autore o di proprietà intellettuale; (V) utilizzare le risorse informatiche per effettuare operazioni non pertinenti all'attività lavorativa;
- la Società deve applicare filtri automatici che prevengono l'accesso a determinati siti reputati non conferenti con l'attività lavorativa, il cui elenco viene periodicamente aggiornato. È vietato rimuovere o tentare di rimuovere i filtri per accedere a siti non consentiti, ed in ogni caso è vietato modificare autonomamente e senza l'autorizzazione dell'Amministratore di Sistema le impostazioni del software di navigazione web (web browser);
- è fatto divieto di intercettare fraudolentemente, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;

- è fatto divieto di 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.

Protocolli specifici di prevenzione

a) Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, account e profili), compreso l'accesso ai sistemi informativi contabili.

Per l'attività sensibile Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, account e profili) compreso l'accesso ai sistemi informativi contabili, 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;
- deve essere prevista 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 esempio, 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;
- deve essere prevista la corretta gestione delle password definita da linee guida, comunicate a tutti gli utenti, per la selezione e l'utilizzo della password;
- la Società è tenuta a custodire in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento;
- è fatto divieto di occultare o distruggere in tutto o in parte e scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari della Società;
- deve essere prevista una verifica periodica da parte della Direzione IT della Capogruppo dei profili abilitati all'utilizzo dei sistemi contabili aziendali rispetto alle modifiche organizzative intervenute finalizzata all'allineamento dei diritti concessi agli users;
- tutti gli accessi ai sistemi informatici devono essere tracciati mediante file di log degli accessi opportunamente salvati e conservati nel rispetto delle normative vigenti;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione delle attività di accesso ai sistemi informatici/ telematici;
- la Società deve svolgere valutazioni approfondite dei rischi per quanto riguarda la sicurezza dei pagamenti via Internet e dei servizi connessi, e a documentarle, sia prima di avviare l'offerta dei servizi sia successivamente con frequenza regolare;

- la Società deve attuare misure di sicurezza in linea con le politiche adottate, al fine di mitigare i rischi individuati. Eventuali minacce ai sistemi di sicurezza sono individuate tramite un sistema di monitoraggio costante dei rischi;
- la Società deve adottare strumenti di sicurezza in grado di proteggere l'interfaccia applicativa resa disponibile all'utente contro l'uso illegale o attacchi informatici;
- periodicamente, indicativamente con cadenza semestrale, il Responsabile Area Business deve relazionare sulla gestione degli incidenti e in generale la gestione del rischio di sicurezza.

b) Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni compreso l'accesso ai sistemi informativi contabili.

Per l'attività sensibile Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni,compreso l'accesso ai sistemi informativi contabili, 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 divulgazionea tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimentoai profili di autorizzazione dei singoli utenti;
- qualora l'attività sia svolta in service da un soggetto il terzo il rapporto deve essereregolato da apposito contratto di servizio;
- devono essere definiti dei criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profiliutente;
- è predisposta una matrice autorizzativa – applicazioni/profili/richiedente – allineata con i ruoli organizzativiin essere e coerente con i principi di segregazione dei ruoli;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione delle attività di accessoai sistemi informatici/ telematici;
- deve essere prevista la verifica periodica dei profili di accesso, di concessione di utenze e della modifica dei profili;
- la Società deve adottare strumenti di sicurezza in grado di proteggere l'interfaccia applicativa resa disponibile all'utente contro l'uso illegale o attacchi informatici;
- nell'ambito del trattamento delle informazioni attraverso sistemi informatici, il controllo degli accessi da parte degli utenti di tali sistemi si realizza attraverso: l'identificazione dell'utente che richiede l'accesso alle informazioni attraverso un identificativo univoco preventivamente assegnatogli; l'autenticazione dell'utente, ovvero la verifica che l'utente sia effettivamente la persona che dichiara di essere; l'autorizzazione dell'utente, ovvero la concessione dell'accesso alle funzionalità e alle informazionirichieste in funzione di un profilo di autorizzazione preventivamente assegnatogli;
- l'Area Sviluppo Prodotti / IT è responsabile dell'intera implementazione delle piattaforme di pagamento online, su cui è possibile effettuare pagamenti via Internet, e dell'implementazione dei controlli di primo livello effettuati sulla stessa.

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 aziendaliinterni, 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;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione dell'installazione dei software applicativi aziendali interni;
- la Società ha definito una metodologia di classificazione delle informazioni in base alla loro criticità e le relative modalità di trattamento in base al livello individuato;
- al fine di proteggere il patrimonio informativo aziendale, la Società ha definito un processo di analisi e gestione dei rischi legati alla sicurezza delle informazioni, in modo tale da garantire che tali informazioni siano adeguatamente protette sulla base della loro effettiva criticità.

d) 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, banchedati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenzae 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;
- i software acquistati dalla Società devono essere catalogati in un apposito database;
- per i software acquistati o comunque in uso da parte della Società, il database comprende anche i seguenti dati:
  - data di acquisto della licenza;
  - data di scadenza della licenza;
  - tipo di utilizzo autorizzato dal contratto di licenza;
- devono essere svolte verifiche periodiche sui software installati al fine di controllare la presenza di softwareproibiti e/o potenzialmente nocivi.

e) 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;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione dell'installazione dei software applicativi aziendali interni;
- la Società ha definito una metodologia di classificazione delle informazioni in base alla loro criticità e le relative modalità di trattamento in base al livello individuato;
- al fine di proteggere il patrimonio informativo aziendale, la Società ha definito un processo di analisi e gestione dei rischi legati alla sicurezza delle informazioni, in modo tale da garantire che tali informazioni siano adeguatamente protette sulla base della loro effettiva criticità.
- la Società ha definito un iter operativo e ruoli e responsabilità relative ai criteri di classificazione delle informazioni aziendali.

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

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, account e profili), compreso l'accesso ai sistemi informativi contabili.			✓	✓			✓							✓	✓	IT - I dipendenti della Società si introducono abusivamente in sistemi informatici esterni al fine di carpire informazioni che possano procurare un interesse o vantaggio alla Società stessa. RIC - La Società investe i proventi derivanti dall'evasione fiscale, resa possibile da una non corretta ricostruzione del reale volume di affari della Società, nell'ambito della propria attività economica (autoriciclaggio). CRI/TSN - Tre o più persone all'interno della Società si associano al fine di commettere un reato rilevante ai sensi del Decreto. TRIB - Attraverso una gestione negligente degli accessi ai sistemi informatici contabili, la Società permette l'occultamento o la distruzione di scritture contabili o documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione del reale volume di affari della società ed evadere le imposte sui redditi o sul valore aggiunto.
Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni, compreso l'accesso ai sistemi informativi contabili.				✓												IT - I dipendenti della Società si introducono abusivamente in sistemi informatici esterni al fine di carpire informazioni che possano 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 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: (i) gestione dell'albo fornitori; (ii) selezione del fornitore e valutazione dei requisiti qualificanti; (iii) stipula di accordi quadro di fornitura; (iv) emissione degli ordini; (v) certificazione dei beni e dei servizi ricevuti.
- 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:

- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25);
- delitti di criminalità organizzata (art. 24-ter);
- 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).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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. In particolare:

- la scelta dei fornitori e la determinazione delle condizioni d'acquisto di beni e servizi è svolta sulla base di criteri obiettivi e imparziali, fondati in prevalenza sulla valutazione della serietà, affidabilità, qualità, efficienza ed economicità;
- la Società si aspetta che fornitori e collaboratori non ricevano alcuna illecita pressione a prestazioni non previste contrattualmente sia in termini di contenuto sia in termini modalità di esecuzione;
- non si possono accettare o ricevere dai fornitori omaggi eccedenti le normali pratiche di cortesia ovvero non in linea con la normale prassi commerciale;
- è fatto obbligo per tutti i fornitori della Società di rispettare gli standard etici e i requisiti di qualifica stabiliti dal Codice Anticorruzione della Società;

- fornitori devono astenersi dal porre in essere condotte corruttive con riferimento a qualunque soggetto con il quale dovessero trovarsi ad operare, sia esso un Pubblico Ufficiale o un privato. In particolare, è vietata qualsiasi condotta o comportamento, contraria ai doveri di diligenza, fedeltà e professionalità, volta ad offrire od ottenere da un Pubblico Ufficiale o da un privato una somma di denaro o altra utilità illegittima o, comunque, non dovuta a fronte dei servizi rispettivamente ricevuti o prestati;

- le attività relative al processo di approvvigionamento sono regolate dalle procedure interne in ambito di Procurement che, in conformità con i principi anticorruzione di cui al presente Codice di Condotta Anticorruzione, definiscono i ruoli e le responsabilità dei principali attori coinvolti e definiscono le regole generali per attività quali la selezione dei fornitori, la definizione e l'aggiornamento dello status di qualifica dei fornitori, l'assegnazione dei contratti, l'inserimento di clausole contrattuali standard di protezione, incluse quelle di impegno al rispetto delle Leggi Anticorruzione e la verifica dei requisiti etici dei fornitori;
- nello svolgimento degli incarichi assegnati, la Società deve stabilire che consulenti esterni e agenti commerciali devono rispettare quanto previsto dal presente Codice e dalle normative nazionali ed internazionali;
- la Società deve valutare adeguatamente i consulenti e gli agenti commerciali, soprattutto in termini di affidabilità e onorabilità, al fine di determinare la ragionevole possibilità che qualcuno di essi possa intraprendere attività proibite dal presente Codice o dalle Leggi Anticorruzione;
- la Società deve effettuare adeguate valutazioni per conoscere la reputazione e l'affidabilità dei propri partner terzi potenziali ed essere in grado di valutare i rischi che possono derivare da attività non in linea con regolamenti interni e/o principi etici definiti da TeamSystem;
- al fine di evitare che, in determinate circostanze TeamSystem possa essere ritenuta responsabile per attività di corruzione commesse dai partners, è fatto obbligo per gli stessi di rispettare gli standard previsti dal Codice Anticorruzione e le disposizioni delle Leggi Anticorruzione;
- TeamSystem si impegna a diffondere tali principi all'interno del Gruppo e a sostenere e promuovere adeguati programmi di compliance per la tutela di TeamSystem e delle società del Gruppo.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

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;**
- **certificazione dei beni e dei servizi ricevuti.**

Per l'attività sensibile 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; certificazione dei beni e dei servizi ricevuti, 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 (ad esempio, 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 (ad esempio, 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 a uniformarsi alle prescrizioni del Codice Etico e del Codice di Condotta Anti Corruzione, nonché alle linee di condotta del Modello 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 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;
- devono essere individuate le scelte in merito al mantenimento della controparte all'interno dell'Albo fornitorio alla relativa cancellazione dalle medesime liste. Tali scelte non possono essere determinate da un unico soggetto e siano sempre motivate;
- deve essere verificato, con riferimento agli acquisti intercompany, che la fornitura di beni o di servizi sia avvenuta a condizioni di mercato;
- deve essere verificata la sussistenza dei requisiti normativi di regolarità della controparte tramite la consegna della documentazione prevista dalla legge (ad esempio, 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 D. Lgs. 231/2001;
- tutte le fatture ricevute devono essere, a fronte di impegni di spesa, formalizzate attraverso un contratto o un ordine di acquisto;
- deve essere accertata la corrispondenza tra il documento di trasporto (DDT) e la quantità di merce ricevuta;
- deve essere accertata la corrispondenza tra l'ordine di acquisto, i beni/ servizi ricevuti la fattura;
- deve essere presente un'adeguata e documentabile giustificazione di tutti i compensi e le somme corrisposte ai Fornitori nel rapporto contrattuale in essere con il fornitore;
- deve essere effettuata un'adeguata attività selettiva dei fornitori al fine di determinare le condizioni d'acquisto di beni e servizi sulla base di valutazioni motivate ed imparziali, fondate sulla qualità, sul prezzo e sulle garanzie fornite;
- devono essere individuati gli indicatori di anomalia per l'identificazione di eventuali transazioni "a rischio" o "sospette" con le controparti;

- devono essere individuati i criteri in base ai quali la controparte può essere cancellata dall'Albo Fornitori della Società;
- nessun rapporto può essere instaurato con persone o enti che non hanno intenzione di adeguarsi ai principi etici della Società, o che rifiutino di impegnarsi al rispetto del Codice Etico e del CodiceAnticorruzione;
- è fatto 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;
- è fatto divieto di utilizzare informazioni su clienti, fornitori, operatori acquisite illecitamente al fine di ottenere benefici di qualunque utilità nelle relazioni commerciali;
- è fatto divieto di effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, oveeccedano le normali pratiche commerciali e di cortesia, a dipendenti di altre società private;
- la scelta dei fornitori deve essere ispirata a criteri di concorrenza, pari opportunità di accesso, competenza,economicità, trasparenza, correttezza, professionalità e tracciabilità delle operazioni effettuate. Il criterio di trasparenza fa riferimento alla precisa individuazione di soggetti responsabili, alla valutazione delle richieste di approvvigionamento, alla verifica che le richieste arrivino da soggetti autorizzati, alla determinazione dei criteri che saranno utilizzati nelle varie fasi del processo. Il principio di economicità nonpuò mai prevalere sugli altri criteri;
- 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 garantita la tracciabilità e trasparenza nella definizione dell'esigenza di acquisto e nell'individuazione del fornitore. Inoltre, il contratto deve chiaramente esplicitare oggetto della fornitura e del servizio e relativi deliverable;
- 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 sussistere i requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e i meccanismi di valutazione complessiva del servizio reso;
- nei contratti con partner, consulenti e professionisti deve essere contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparatiin procedimenti giudiziari relativi ai reati contemplati dalla presente Parte Generale;
- per le spese che per loro natura e per l'importo contenuto (c.d. piccole spese) risultano più facilmente gestibili attraverso un processo semplificato rispetto a quello standard di ciclo passivo si procede come specificato nelle rispettive procedure interne;
- deve essere garantita la raccolta delle informazioni relative ai fornitori e del loro inserimento nel sistema amministrativo contabile (ad esempio, nome cliente/ fornitore; indirizzo: via, località, paese, regione; partitaIVA;conto di riconciliazione);
- devono essere processate dalle Aree competenti solo le richieste di apertura, integrazione, modifica o cancellazione di un'anagrafica (fornitori - clienti) corredate da idonea documentazione di supporto;
- devono essere previsti controlli sull'anagrafica fornitori in relazione alla creazione/ variazione di campi anagrafici chiave (coordinate bancarie, partita IVA, etc.);
- devono essere previsti controlli sulla qualificazione del fornitore (identità pregressa nell'albo fornitori, verifiche sulla qualità della prestazione resa, etc.);
- devono essere previsti controlli sull'iter d'approvazione degli ordini di acquisto e sugli approval limits;
- devono essere previsti controlli su eventuali ordini non processati con ordine di acquisto o al di fuori delle procedure autorizzative standard (ad esempio, piccole spese);
- la certificazione delle prestazioni ricevute (beni e servizi) per importi superiori a quanto previstocontrattualmente può essere effettuata solo in presenza di modifiche contrattuali valide;

- in fase di stipula del contratto deve essere formalmente nominato un gestore amministrativo del contratto incaricato della verifica e gestione durante l'esecuzione degli aspetti di carattere amministrativo. Inoltre, il contratto deve chiaramente esplicitare oggetto della fornitura e del servizio e relativi deliverable;
- la Società ha adottato una procedura che descrive ruoli, compiti e responsabilità ai fini della selezione, gestione e controllo dei fornitori strategici;
- l'Amministratore Delegato verifica e approva la richiesta di acquisto/il documento contenente tutte le informazioni dettagliate per l'individuazione della fornitura, inviata dal Referente del Contratto (in caso di fornitura standard) o dal Referente delle Attività Esternalizzate (in caso di fornitura strategica);
- il Consiglio di Amministrazione deve esaminare e approvare la richiesta di classificazione come fornitore strategico, opportunamente motivata;
- la documentazione accompagnatoria o comunque relativa alla fornitura/contratto di esternalizzazione deve essere archiviata dalle Aree/ Funzioni interessate e dall'Area Amministrazione, Finanza e Controllo;
- il Referente delle Attività Esternalizzate annualmente deve redigere un documento che contiene la sintesi dell'operato dei fornitori strategici nel periodo di riferimento ed i risultati che sono stati raggiunti. Il documento viene inviato all'Amministratore Delegato.

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:

- 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 (ad esempio, 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 (ad esempio, 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 dei consulenti esterni ad uniformarsi alle prescrizioni del Codice Etico e del Codice Anticorruzione, nonché alle linee di condotta del Modello 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 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;
- devono essere individuate le scelte in merito al mantenimento della controparte all'interno dell'Albo fornitorio alla relativa cancellazione dalle medesime liste non possano essere determinate da un unico soggetto e siano sempre motivate;

- deve essere verificato, con riferimento agli acquisti intercompany, che la fornitura di beni o di servizi sia avvenuta a condizioni di mercato;
- deve essere verificata sulla sussistenza dei requisiti normativi di regolarità della controparte tramite la consegna della documentazione prevista dalla legge (ad esempio, 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;
- deve essere presente un'adeguata e documentabile giustificazione di tutti i compensi e le somme corrisposte ai fornitori nel rapporto contrattuale in essere con il fornitore;
- deve essere effettuata 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;
- devono essere individuati gli indicatori di anomalia per l'identificazione di eventuali transazioni "a rischio" o "sospette" con le controparti;
- devono essere individuati i criteri in base ai quali la controparte può essere cancellata dall'Albo Fornitori della Società;
- la scelta dei fornitori deve essere ispirata a criteri di concorrenza, pari opportunità di accesso, competenza, economicità, trasparenza, correttezza, professionalità e tracciabilità delle operazioni effettuate. Il criterio di trasparenza fa riferimento alla precisa individuazione di soggetti responsabili, alla valutazione delle richieste di approvvigionamento, alla verifica che le richieste arrivino da soggetti autorizzati, alla determinazione dei criteri che saranno utilizzati nelle varie fasi del processo. Il principio di economicità non può mai prevalere sugli altri criteri;
- 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 effettuata un'adeguata attività selettiva fra i diversi operatori di settore; in assenza di un'attività selettiva tra diversi operatori del settore, sia data un'evidenza formale delle ragioni della deroga ed esecuzione da parte del responsabile di una valutazione sulla congruità del compenso pattuito (rispetto agli standard di mercato);
- 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 sussistere i requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e i meccanismi di valutazione complessiva del servizio reso;
- nei contratti con partner, consulenti e professionisti deve essere contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparati in procedimenti giudiziari relativi ai reati contemplati dalla presente Parte Generale;
- deve essere garantita la tracciabilità e trasparenza nella definizione dell'esigenza di acquisto e nell'individuazione del fornitore;
- deve essere accertata corrispondenza tra ordine di acquisto, beni/servizi ricevuti e la relativa fattura;
- al termine dell'incarico deve essere richiesto al consulente di dettagliare per iscritto le prestazioni effettuate;
- il rapporto tra la Società e il consulente 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;
- deve essere garantita la raccolta delle informazioni relative ai fornitori e del loro inserimento nel sistema amministrativo contabile (ad esempio, nome cliente/fornitore; indirizzo: via, località, paese, regione; partita IVA; conto di riconciliazione);

- devono essere processate dalle Aree/ Funzioni competenti solo le richieste di apertura, integrazione, modifica o cancellazione di un'anagrafica (fornitori - clienti) corredate da idonea documentazione di supporto;
- devono essere previsti controlli sull'anagrafica fornitori in relazione alla creazione/ variazione di campi anagrafici chiave (coordinate bancarie, partita IVA, etc.);
- devono essere previsti sulla qualificazione del fornitore (identità pregressa nell'albo fornitori, verifiche sulla qualità della prestazione resa, etc.):
- devono essere previsti controlli sull'iter d'approvazione degli ordini di acquisto e sugli approval limits;
- devono essere previsti controlli su eventuali ordini non processati con ordine di acquisto o al di fuori delle procedure autorizzative standard (ad esempio, piccole spese);
- la certificazione delle prestazioni ricevute (beni e servizi) per importi superiori a quanto previstocontrattualmente può essere effettuata solo in presenza di modifiche contrattuali valide;
- in fase di stipula del contratto deve essere formalmente nominato un gestore amministrativo del contrattoincaricato della verifica e gestione durante l'esecuzione degli aspetti di carattere amministrativo. Inoltre, ilcontratto deve chiaramente esplicitare oggetto della fornitura e del servizio e relativi deliverable.
- tutte le fatture ricevute devono essere, a fronte di impegni di spesa, formalizzate attraverso un contratto oun ordine di acquisto;
- deve essere accertata corrispondenza tra ordine di acquisto, beni/servizi ricevuti e la relativa fattura;
- la Società ha adottato una procedura che descrive ruoli, compiti e responsabilità ai fini della selezione,gestione e controllo dei fornitori strategici;
- l'Amministratore Delegato verifica e approva la richiesta di acquisto/il documento contenente tutte le informazioni dettagliate per l'individuazione della fornitura, inviata dal Referente del Contratto (in caso di fornitura standard) o dal Referente delle Attività Esternalizzate (in caso di fornitura strategica);
- il Consiglio di Amministrazione deve esaminare e approvare la richiesta di classificazione come fornitore strategico, opportunamente motivata;
- la documentazione accompagnatoria o comunque relativa alla fornitura/contratto di esternalizzazione deve essere archiviata dalle Aree/ Funzioni interessate e dall'Area Amministrazione, Finanza e Controllo;
- il Referente delle Attività Esternalizzate annualmente deve redigere un documento che contiene la sintesidell'operato dei fornitori strategici nel periodo di riferimento ed i risultati che sono stati raggiunti. Il documento viene inviato all'Amministratore Delegato.

Area di rischio: Approvvigionamento di beni e servizi

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
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; - certificazione dei beni e dei servizi ricevuti..	✔	✔	✔				✔					✔		✔	✔	PA - La Società offre denaro a pubblici ufficiali al fine di garantire la stipula, a condizioni economiche particolarmente favorevoli per la stessa, di un accordo per la fornitura di servizi con una società partecipata da un Ente Pubblico SOC/CP - La Società offre denaro o altra utilità al legale rappresentante di una società privata affinché accetti la stipula, a condizioni economiche particolarmente favorevoli per la Società, di un accordo commerciale per la fornitura di beni e/o servizi RIC - La Società acquista beni sottocosto poiché provenienti da attività illecite o investe i proventi derivanti da attività corruttive nell'acquisto di beni (autoriciclaggio). 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. TRIB - La Società stipula contratti di acquisto di beni o servizi inesistenti, al solo fine di registrare elementi passivi fittizi ed evadere le imposte sui redditi o sul valore aggiunto.
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 Pubblica Amministrazione al fine di ottenere indebiti vantaggi. SOC/CP - La Società corrompe la controparte al fine di stipulare contratti di acquisto a un prezzo inferiore a quello di mercato. 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. TRIB - La Società stipula contratti di acquisto di beni o servizi inesistenti, al solo fine di registrare elementi passivi fittizi ed evadere le imposte sui redditi o sul valore aggiunto.

SEZIONE I – Prestazione dei servizi di pagamento

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 prestazione dei servizi di pagamento, ed in particolare alle attività sensibili:

- Gestione dei rapporti con clienti diretti – privati (fornitura dei servizi di incasso, PIS e AIS) con particolare riferimento alle seguenti attività: (i) gestione dell'anagrafica cliente (adeguata verifica della clientela ai fini antiriciclaggio, etc.); (ii) definizione delle condizioni economiche in deroga; (iii) sottoscrizione dei contratti dei servizi prestati; (iv) assistenza della clientela in corso di rapporto;
- Gestione dei rapporti con clienti diretti – Pubbliche Amministrazioni A (fornitura dei servizi di incasso, PIS e AIS);
- Gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi con particolare riguardo ai clienti e distributori.
- Gestione e utilizzo di strumenti di pagamento diversi da i contanti.

Reati applicabili

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

- indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24);
- delitti informatici e trattamento illecito dei dati (art. 24-bis);
- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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);
- reati tributari (art. 25-quinquiesdecies);
- reati transnazionali (art. 10, L. 146/2006).
- indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (Art. 25-octies. 1);
- detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti Art. 25-octies. 1);
- frode informatica" nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (Art. 25-octies. 1);
- delitti contro il patrimonio culturale (25-septiesdecies);
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (25-duodeviecies).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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 della prestazione dei servizi di pagamento. In particolare:

- i rapporti con i clienti devono essere condotti con correttezza, trasparenza e imparzialità e da personale qualificato;
- la Società si aspetta anche dai clienti, debitamente informati da TeamSystem, comportamenti conformi ai principi contenuti nel presente Codice Etico. Comportamenti diversi possono essere considerati grave inadempimento ai doveri di correttezza e buona fede nell'esecuzione del contratto, motivo di lesione del rapporto fiduciario e giusta causa di risoluzione dei rapporti contrattuali;
- TeamSystem richiede che i rapporti con le terze parti – fornitori, clienti, consulenti, e altre persone fisiche, persone giuridiche (anche appartenenti allo stesso Gruppo TeamSystem) ed enti di fatto – intrattenuti durante lo svolgimento delle attività di business, siano improntati a criteri di massima correttezza, trasparenza e tracciabilità delle fonti informative, nonché nel rispetto delle Leggi Anticorruzione e di tutte le altre leggi applicabili;
- la Società definisce chiaramente ai diversi livelli, i ruoli, i compiti e le responsabilità facendo riferimento alle procedure societarie intese a garantire l'osservanza degli obblighi antifrode e di adeguata verifica della clientela, di segnalazione delle operazioni sospette, di conservazione della documentazione e delle evidenze dei rapporti e delle operazioni;
- nell'ambito dei rapporti con la Pubblica Amministrazione., è necessario prestare particolare cura nel non porre in essere atti in violazione delle prescrizioni di legge e del presente Codice Etico. In particolare, è fatto espresso divieto di:
    - 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, etc. e richieste di finanziamenti, contributi, sovvenzioni ed erogazioni dallo Stato o altro soggetto appartenente alla Pubblica Amministrazione;
    - procurare indebitamente qualsiasi altro tipo di profitto (licenze, autorizzazioni, sgravi di oneri, anche previdenziali, etc.) con mezzi che costituiscano artifici o raggiri (per esempio invio di documentazione non veritiera);
    - influenzare in alcun modo le decisioni di rappresentanti della Pubblica Amministrazione in maniera impropria e/o illecita (come, a titolo di esempio, sollecitare e/o accettare e/o corrispondere e/o offrire a imedesimi, direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per sé o per la Società). Atti di cortesia commerciale (come, a titolo di esempio, omaggi o forme di ospitalità) sono consentiti solo se non eccedono le normali pratiche commerciali e/o di cortesia e se, in ogni caso, sono tali da non compromettere l'imparzialità e l'indipendenza di giudizio del rappresentante della Pubblica Amministrazione;
    - 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.

È, altresì, fatto espresso divieto di:

- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva); quando

l'intenzione sia:

- indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di natura pubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
- influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;

- influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio;
- ottenere, assicurarsi o mantenere un business o un ingiusto vantaggio in relazione alle attività d'impresa; o in ogni caso, violare le leggi applicabili.

La condotta proibita include l'offerta a, o la ricezione da parte di, il personale della Società (corruzione diretta) o chiunque agisca per conto di TeamSystem (corruzione indiretta) di un vantaggio economico o altra utilità in relazione alle attività di impresa svolte nello svolgimento delle proprie mansioni lavorative e professionali.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

Protocolli specifici di prevenzione

a) Gestione dei rapporti con clienti diretti – privati (fornitura dei servizi di incasso, PIS e AIS) con particolare riferimento alle seguenti attività:

- **gestione dell'anagrafica cliente (adeguata verifica della clientela ai fini antiriciclaggio, etc.);**
- **definizione delle condizioni economiche in deroga;**
- **sottoscrizione dei contratti dei servizi prestati**
- **assistenza della clientela in corso di rapporto.**
- Per l'attività sensibile gestione dei rapporti con clienti diretti – privati (fornitura dei servizi di incasso, PIS e AIS) con particolare riferimento alle seguenti attività: gestione dell'anagrafica cliente (adeguata verifica della clientela ai fini antiriciclaggio, etc.); definizione delle condizioni economiche in deroga; sottoscrizione dei contratti dei servizi prestati; assistenza della clientela in corso di rapporto, i protocolli prevedono che:

- gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto dai soggetti appositamente incaricati;
- il sistema dei poteri e delle deleghe deve stabilire le facoltà di autonomia gestionale per natura di impegno;
- le attività di sviluppo commerciale devono essere svolte da strutture diverse rispetto a quelle che gestiscono operativamente l'erogazione dei servizi contrattualizzati;
- la definizione delle condizioni economiche contrattuali deve essere esclusivamente affidata al Responsabile dell'Area aziendale competente; l'atto formale di sottoscrizione avviene in base al vigente sistema dei poteri e delle deleghe;
- la documentazione relativa al contratto deve essere sottoposta per il controllo al Responsabile dell'Area competente che si avvale delle strutture a supporto a ciò preposte;
- ogni contratto deve essere formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Area è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta e raccolta, nonché della modulistica sottoscritta;
- è fatto divieto di emettere fatture o rilasciare documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- i contratti stipulati con le controparti devono essere predisposti in forma scritta e coerentemente con i format contrattuali approvati dalla Società e l'oggetto della prestazione deve essere chiaramente individuato;
- preventivamente alla sottoscrizione di offerte commerciali e alla "stipula contrattuale" deve essere eseguita una verifica sulle controparti ai fini di valutare il rischio associato;

- la sottoscrizione del contratto deve avvenire da parte del soggetto procurato sulla base delle verifiche amministrative svolte e in presenza della documentazione che attesti la richiesta da parte del potenziale cliente, della coerenza della prestazione offerta con il business aziendale, l'approvazione degli adeguati livelli di condizioni particolari e/o scontistiche;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione dell'on boarding della clientela;
- i contratti devono essere redatti in forma scritta o con documento informatico che soddisfi i requisiti della forma scritta;
- la Società ha adottato un processo operativo al fine di assicurare che la documentazione fornita alla clientela rispetti le Disposizioni di Vigilanza relative alla predisposizione di un nuovo prodotto/servizio;
- tutte le evidenze del processo di contrattualizzazione devono essere archiviate nelle apposite cartelle informatiche o fisiche, in modo che sia sempre possibile attestare che il processo definito sia stato rispettato;
- la Società ha istituito adeguati presidi organizzativi e procedurali al fine di prevenire e impedire la realizzazione di operazioni di riciclaggio e di finanziamento al terrorismo. Inoltre, deve assicurarsi che nella struttura organizzativa siano rispettate le norme a tutela della prevenzione del riciclaggio e del finanziamento del terrorismo;
- in aderenza all'approccio basato sul rischio, le politiche di governo dei rischi connessi con il riciclaggio devono essere adeguate all'entità e alla tipologia dei rischi cui è concretamente esposta l'attività della Società, come rappresentati nel documento di valutazione dei rischi;
- la Società è tenuta a seguire l'iter procedurale per corretto adempimento degli obblighi in materia di antiriciclaggio e antiterrorismo, che prevede l'adeguata verifica della clientela nonché un monitoraggio costante della relazione per gli ambiti di propria competenza.

b) Gestione dei rapporti con clienti diretti Pubbliche Amministrazioni (fornitura dei servizi di incasso, PIS e AIS)

Per l'attività sensibile gestione dei rapporti con clienti diretti Pubbliche Amministrazioni (fornitura dei servizi di incasso, PIS e AIS), i protocolli prevedono che:

- i soggetti che esercitano poteri autorizzativi e/o nei confronti della Pubblica Amministrazione sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal sistema delle deleghe aziendale;
- gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto dai soggetti appositamente incaricati;
- il sistema dei poteri e delle deleghe deve stabilire le facoltà di autonomia gestionale per natura di impegno, ivi incluse quelle nei confronti della Pubblica Amministrazione;
- le attività di sviluppo commerciale devono essere svolte da strutture diverse rispetto a quelle che gestiscono operativamente l'erogazione dei servizi contrattualizzati;
- la definizione delle condizioni economiche contrattuali deve essere esclusivamente affidata al Responsabile dell'Area aziendale competente; l'atto formale di sottoscrizione avviene in base al vigente sistema dei poteri e delle deleghe;
- la documentazione relativa al contratto deve essere sottoposta per il controllo al Responsabile dell'Area competente che si avvale delle strutture a supporto a ciò preposte;
- ogni sottoscrizione deve essere formalizzata in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Area è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta e raccolta, nonché della modulistica sottoscritta;
- tutta la documentazione predisposta dalla Società per l'accesso a bandi di gara pubblici deve essere verificata, in termini di veridicità e congruità sostanziale e formale, dal Responsabile dell'Area aziendale competente;
- ciascuna fase rilevante degli accordi con la Pubblica Amministrazione deve risultare da apposita documentazione scritta;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Area è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via

telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione;

- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione dell'on boarding della clientela;
- i contratti devono essere redatti in forma scritta o con documento informatico che soddisfi i requisiti della forma scritta;
- la Società ha adottato un processo operativo al fine di assicurare che la documentazione fornita alla clientela rispetti le Disposizioni di Vigilanza relative alla predisposizione di un nuovo prodotto/servizio;
- tutte le evidenze del processo di contrattualizzazione devono essere archiviate nelle apposite cartelle informatiche o fisiche, in modo che sia sempre possibile attestare che il processo definito sia stato rispettato;
- la Società ha istituito adeguati presidi organizzativi e procedurali al fine di prevenire e impedire la realizzazione di operazioni di riciclaggio e di finanziamento al terrorismo. Inoltre, deve assicurarsi che nella struttura organizzativa siano rispettate le norme a tutela della prevenzione del riciclaggio e del finanziamento del terrorismo;
- in aderenza all'approccio basato sul rischio, le politiche di governo dei rischi connessi con il riciclaggio devono essere adeguate all'entità e alla tipologia dei rischi cui è concretamente esposta l'attività della Società, come rappresentati nel documento di valutazione dei rischi;
- la Società è tenuta a seguire l'iter procedurale per corretto adempimento degli obblighi in materia di antiriciclaggio e antiterrorismo, che prevede l'adeguata verifica della clientela nonché un monitoraggio costante della relazione per gli ambiti di propria competenza.

c) 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:

- nella fase di studio di fattibilità del progetto devono essere valutati possibili conflitti con titoli di proprietà altrui;
- deve essere assicurata la possibilità di ricostruire tutte le fasi che hanno portato allo sviluppo di un nuovo servizio/ software;
- i processi autorizzativi devono essere sempre accuratamente documentati e verificabili a posteriori;
- devono essere elaborate clausole riferite all'osservanza anche da parte dei terzi contraenti delle norme in materia di proprietà intellettuale;
- devono essere controllati i mezzi di comunicazione interni ed esterni alla società (ad esempio, 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 D. Lgs. 231/2001;
- devono essere 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, devono 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 sia sempre prevista una clausola che preveda il diritto di autore e tutela della società;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione della sicurezza dei pagamenti via internet;
- per quanto riguarda la sicurezza dei pagamenti via Internet e dei servizi connessi, la Funzione Risk Management svolge un'attività di analisi dei rischi con periodicità almeno annuale e provvede all'aggiornamento della stessa in caso di modifiche di una certa entità (che abbiano un impatto rilevante sui processi IT che presidiano il business), avvalendosi dei contributi dell'attività della Funzione Sviluppo Prodotti/ IT. I risultati di tali analisi sono a disposizione della Funzione Risk Management per opportuna condivisione;

- la Società adotta strumenti di sicurezza in grado di proteggere l'interfaccia applicativa resa disponibile all'utente contro l'uso illegale o attacchi informatici;
- ogni utente è tenuto a inserire una username e una password, scelte in fase di registrazione. Per garantire una maggiore sicurezza in fase di registrazione, è posto un vincolo per l'utente in merito alla complessità della password;
- periodicamente, indicativamente con cadenza semestrale, il Responsabile Area Business relaziona sulla gestione degli incidenti e in generale la gestione del rischio di sicurezza;
- in caso di incidenti di sicurezza le unità organizzative interessate danno comunicazione all'Amministratore Delegato e al Consiglio di Amministrazione, nonché all'Autorità competente.
- per ogni nuovo prodotto la Società deve adottare un processo standard di predisposizione di un nuovo prodotto /servizio che prevede la definizione e la fattibilità del nuovo prodotto da parte del Responsabile Area Business;
- una volta definito e approvato il nuovo prodotto il Responsabile Area Business, con l'ausilio della Funzione Legale, dovrà predisporre la documentazione prevista conforme alla normativa vigente;
- la Società ha definito nella normativa interna il processo operativo che ha adottato al fine di assicurare che la documentazione fornita alla clientela rispetti le Disposizioni di Vigilanza relative alla predisposizione di un nuovo prodotto/servizio;
- la Società ha definito un iter operativo e ruoli e responsabilità relativi allo sviluppo di applicazioni sicure nell'ambito dello sviluppo software, al fine di minimizzare gli impatti sul business e raggiungere gli obiettivi di sicurezza prefissati.

d) Gestione e utilizzo di strumenti di pagamento diversi dal contante.

Per l'attività sensibile gestione e utilizzo di strumenti di pagamento diversi dal contante, i protocolli prevedono che:

- la Società debba essere dotata di procedure che definiscano ruoli e responsabilità relativi alla gestione della sicurezza dei pagamenti via internet nel rispetto del principio della separazione dei compiti. La procedura "On Boarding" individua i soggetti che, per le rispettive competenze, sono tenuti ad interagire nell'ambito della prestazione dei servizi di pagamento. La procedura antifrode individua i soggetti che sono responsabili delle attività di monitoraggio e prevede che debba essere approntato un sistema di alerting automatico che viene registrato sui sistemi;
- venga rispettato il principio della tracciabilità in forza del quale ogni processo deve essere adeguatamente documentato, motivato ed approvato, che la documentazione sia archiviata, in formato cartaceo e/o elettronico, presso le Funzioni competenti;
- si riuniscano periodicamente il responsabile Business, il responsabile Customer Care, la funzione AML, la funzione Antifrode e la responsabile Antifrode per discutere sugli esiti delle attività di monitoraggio antifrode e decidere sulle eventuali azioni da intraprendere e presidi da adottare. Gli esiti delle riunioni periodiche confluiscono in un report di monitoraggio frodi trimestralmente prodotto dalla Funzione Antifrode;
- vi sia un sistema di controlli di sicurezza sui sistemi di accesso agli applicativi messi a disposizione della propria clientela che riguarderà principalmente i log di accesso e la verifica di eventuali operazioni fraudolente;
- i sistemi antifrode connessi al servizio di Incasso dispongano di un set di regole predefinite dai sistemi di Stripe per il blocco di default delle operazioni e la struttura Antifrode effettui una verifica in Black List per gli IBAN di accredito;
- i sistemi antifrode del servizio PIS abbiano:
  - definito l'invio di una notifica al Merchant via email ad ogni disposizione PIS;
  - un blocco alla possibilità di disporre pagamenti tramite PIS laddove il medesimo pagamento sia già stato eseguito con successo;
  - stabilito un limite giornaliero di disposizioni PIS per Merchant;
  - un controllo sulla frequenza delle disposizioni PIS (es. non consentito eseguire più PIS nell'arco di 1 min);
- Sistemi Antifrode Servizio AIS abbiano:
  - un limite alla frequenza di consensi consentiti (es. non consentito eseguire più di un nuovo consenso nell'arco di 5 secondi);
  - un controllo sulla revoca del consenso;

- una notifica al Merchant via email ad ogni aggiunta/rinnovo del consenso ovvero all'accesso tramite SCA ai conti indicati;

- la struttura Antifrode, in sede di controllo giornaliero, verifichi gli alert giornalieri scattati automaticamente sulla base dei KPI-FRODI presenti nella sezione dedicata del Portale TS Pay . Per ogni servizio la Procedura Antifrode prevede un monitoraggio specifico;
- le attività siano sottoposte a verifica dalla funzione Internal Audit.

Area di rischio: Prestazione dei servizi di pagamento

	Categorie di reato																	
Attività sensibili	PA	SOC/CP	RIC	IT	IND	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	FROD	RIC BEN CUL	Esempio di reato
Gestione dei rapporti con clienti diretti – privati (fornitura dei servizidi incasso, PIS e AIS) con particolare riferimento alle seguenti attività: - gestione dell'anagrafica cliente (adeguata verifica della clientela ai fini antiriciclaggio, etc.); - definizione delle condizioni economiche in deroga; - sottoscrizionedei contratti deiservizi prestati assistenza della clientela in corso di rapporto.		✔	✔				✔							✔	✔		✔	SOC/CP - La Società condiziona indebitamente i clienti privati (persone fisiche o rappresentanti di persone giuridiche), offrendo o promettendo utilità improprie, al fine di vendere i propri servizi di pagamento. RIC- La Società, non avendo accertato l'identità della controparte, presta servizi di pagamento ricevendo consapevolmente somme di denaro di provenienza delittuosa. CRI/TSN - La Società presta servizi di pagamento a clienti legati ad associazioni criminali. TRIB - La Società emette o rilascia fatture o altri documenti per operazioni inesistenti a soggetti terzi al fine di consentirne l'evasione fiscale. RIC BEN CUL - un soggetto apicale o sottoposto della Società agevoli un cliente (operante nel mondo dell'arte) nell'attività di re-immissione nel circuito legale di denaro o altri beni di provenienza illecita per il tramite di servizi di pagamento offerti dalla Società, non adempiendo agli obblighi antiriciclaggio.
Gestione dei rapporti con clienti diretti – Pubbliche Amministrazioni (fornitura dei servizi di incasso, PIS eAIS).	✔																	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 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 a procurarsi informazioni dei clienti al fine di ottenere un vantaggio. DA - La Società nell'ambito della attività di progettazione potrebbe astrattamente sviluppare SW sfruttando indebitamente proprietà intellettuale altrui. FA - La Società commercializza software il cui marchio risulta contraffatto.
Gestione e utilizzo di strumenti di pagamento diversi dal contante.																✔		IT – Un dipendente nell'interesse e vantaggio della Società effettui un accesso abusivo a sistema telematico al fine di commettere una transazione non autorizzata.

																	FROD - La Società mettendo a disposizione strumenti di pagamento diversi dal contante agevoli la clientela a commettere un reato di frode ovvero, un dipendente, utilizzando uno strumento di pagamento diverso dal contante, effettui una transazione non autorizzata nell'interesse o a vantaggio della Società.

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 (ad esempio, accordi di collaborazione per la "commercializzazione" dei servizi di pagamento) con particolare riferimento alle seguenti attività: (i) individuazione delle opportunità di partnership commerciali; (ii) 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:

- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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 tributari (art. 25-quinquiesdecies);
- reati transnazionali (art. 10, L. 146/2006).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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*.

In particolare, è fatto divieto di:

- offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra utilità ad un Pubblico Ufficiale o ad un privato (corruzione attiva);
- accettare la richiesta da, o sollecitazioni da, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, un vantaggio economico o altra utilità da chiunque (corruzione passiva);

quando l'intenzione sia:

- indurre un Pubblico Ufficiale o un privato, a esercitare in maniera impropria qualsiasi funzione di natura pubblica o comunque incentrata sulla buona fede nell'esercizio delle proprie responsabilità affidategli in modo fiduciario in un rapporto professionale anche per conto di soggetti privati terzi, o a svolgere qualsiasi attività associata ad un business ricompensandolo per averla svolta;
- influenzare un atto ufficiale (o una omissione) da parte di un Pubblico Ufficiale o qualsiasi decisione in violazione di un dovere d'ufficio anche da parte di soggetti privati;
- influenzare o compensare un Pubblico Ufficiale o un privato per un atto del suo ufficio.

Inoltre, TeamSystem richiede che i rapporti con le terze parti – fornitori, clienti, consulenti, e altre persone fisiche, persone giuridiche (anche appartenenti allo stesso Gruppo TeamSystem) ed enti di fatto – intrattenuti durante lo svolgimento delle attività di business, siano improntati a criteri di massima correttezza, trasparenza e tracciabilità delle fonti informative, nonché nel rispetto delle Leggi Anticorruzione e di tutte le altre leggi applicabili.

Infine, TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo che è proibito il ricorso a qualsiasi forma di pagamento illecito, in denaro o altra utilità (tutto ciò che rappresenta un vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque già dovute da parte di soggetti suoi interlocutori.

Protocolli specifici di prevenzione

a) Gestione dei rapporti con società private con le quali si intende stipulare accordi di partnership (ad esempio, accordi di collaborazione per la "commercializzazione" dei servizi di pagamento), con particolare riferimento alle seguenti attività:

- **individuazione delle opportunità di partnership commerciali;**
- **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 (ad esempio, accordi di collaborazione per la "commercializzazione" dei servizi di pagamento), con particolare riferimento alle attività di individuazione delle opportunità di partnership commerciali; definizione degli accordi con i partner, i protocolli prevedono che:

- nella fase di "Contrattualizzazione", i contratti redatti in collaborazione con funzione legale devono: (i) essere definiti avendo a riferimento i prezzi medi di mercato applicati al servizio oggetto di acquisto; (ii) 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; (iii) 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 prevista l'effettuazione di periodica attività valutativa circa la qualità del servizio reso e della rispondenza dei soggetti ai requisiti di selezione;
- 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 deve essere 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 ne sia acquisito, per le persone fisiche, il casellario giudiziale o una relativa autocertificazione ove compatibile con la normativa sulla protezione dei dati personali;

- 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 Anticorruzione;
- devono essere svolti controlli formali sulla presenza di precedenti penali ed eventuali comportamenti non conformi al Codice Etico e del Codice di Anticorruzione della Società partner;
- devono essere effettuate verifiche in merito a possibili conflitti di interesse con la Pubblica Amministrazione;
- devono essere definiti adeguati livelli autorizzativi (in coerenza con il sistema di procure aziendali) per la stipulazione dei contratti, listini, campagne, prestazioni etc.;
- deve essere garantita la tracciabilità della documentazione attraverso i sistemi gestionali di cui la Società si è dotata;
- i contratti con partner internazionali devono essere formalmente approvati dall'Amministratore Delegato oda un soggetto dotato di idonei poteri, e le clausole contrattuali, vengono stipulate in collaborazione con l'Ufficio Legale;
- i partner devono essere preventivamente verificati, attraverso l'analisi delle visure che garantiscono di ottenere informazioni utili e valutarne la solidità economica prima di avviare rapporti d'affari;
- devono essere 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 (ad esempio, SLA d'ingaggio);
- è fatto 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;
- anche la scelta dei partner ricade su operatori che rispondono a criteri di eticità, affidabilità, buona reputazione, credibilità nel mercato di riferimento e serietà professionale;
- la Società richiede massima trasparenza nelle operazioni commerciali e nei rapporti con i terzi, nel pieno rispetto delle normative, nazionali e internazionali, in tema di lotta al fenomeno del riciclaggio;
- i Destinatari non possono di conseguenza avviare rapporti d'affari per conto della Società con partner o fornitori o terzi che non diano adeguate garanzie di onorabilità e non godano di buona reputazione ovveroil cui nome sia associato a vicende connesse ad attività di riciclaggio;
- tutte le transazioni finanziarie devono trovare adeguata giustificazione nei rapporti contrattuali e devono essere effettuate mediante mezzi di pagamento che ne garantiscano la tracciabilità.
- la Società dovrà intrattenere rapporti d'affari esclusivamente con clienti e fornitori di sicura reputazione, che svolgono attività commerciali lecite e i cui proventi derivano da fonti legittime. Ciascuna unità aziendale dovrà dotarsi di misure idonee a garantire che non siano accettate forme di pagamento identificate qualestrumento di riciclaggio di denaro illecito. La Società è impegnata al pieno rispetto di tutte le leggi antiriciclaggio vigenti a livello internazionale, comprese quelle che prescrivono la denuncia di transazioni sospette in denaro contante o di altra natura.

Area di rischio: Gestione delle partnership.

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione dei rapporti con società private con le quali si intende stipulare accordi di partnership (ad esempio, accordi di collaborazione per la "commercializzazione" dei servizi di pagamento) con particolare riferimento alle seguenti attività: - individuazione delle opportunità di partnership commerciali; - definizione degli accordi con i partner.	✔	✔	✔				✔							✔	✔	PA - La Società offre denaro a pubblici ufficiali al fine di garantire la stipula, a condizioni economiche particolarmente favorevoli per la stessa, di un accordo di partnership con una società partecipata da un Ente Pubblico. SOC/CP - La Società condiziona indebitamente corruzione del legale rappresentante di un potenziale collocatore affinché quest'ultimo stipuli un contratto per il collocamento dei prodotti della Società a condizioni particolarmente vantaggiose per quest'ultima, al fine di incrementare i volumi di vendita della Società mantenendo basse le commissioni corrisposte al collocatore RIC - La Società non ha previsto o non prevede e/o verifica, in fase di stipula di rapporti contrattuali per il collocamento di prodotti nonché nel corso del rapporto stesso, l'adozione da parte dei collocatori di adeguate procedure e presidi di controllo in materia di antiriciclaggio volti alla corretta identificazione e verifica della clientela CRI/TSN - La Società stipula accordi di partnership con agenti, partner commerciali legati ad associazioni criminali TRIB - La Società emette o rilascia fatture o altri documenti per operazioni inesistenti a soggetti terzi al fine di consentirne l'evasione fiscale.

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, e in particolare alle attività sensibili:

- Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standardtecnico-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 etc.);
- 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 dilegge.

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 gravi o 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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, che costituiscono parte integrantedello 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 conformialla 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. In particolare;

- TeamSystem, consapevole dell'importanza di garantire le migliori condizioni di salute e sicurezza negli ambienti di lavoro, si impegna a promuovere e diffondere tra i propri dipendenti comportamenti responsabili, mettendo in atto le necessarie azioni preventive, al fine di preservare la salute, la sicurezzae l'incolumità di tutto il personale nonché dei terzi che frequentano i propri locali;

- la cultura della salute e sicurezza viene diffusa in modo sistematico, attraverso momenti formativi e di comunicazione, e si realizza mediante un continuo aggiornamento delle metodologie e dei sistemi, alla luce delle migliori tecnologie disponibili, effettuando un'analitica valutazione dei rischi, delle criticità dei processi e delle risorse da proteggere;
- gli esponenti aziendali che ricoprono ruoli sensibili ai fini della salute e sicurezza si impegnano al rispetto delle norme e degli obblighi da questo derivanti in tema di prevenzione e protezione ponendosi, comunque, obiettivi di eccellenza che vanno oltre il mero adempimento, nella piena consapevolezza del valore rappresentato dalla salvaguardia delle condizioni di salute, sicurezza e benessere della persona.

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 rispettodegli standard tecnico-strutturali, i protocolli prevedono che:

- la conformità alle vigenti norme in materia (leggi, norme tecniche e regolamenti, etc.) deve essere assicurata attraverso l'adozione di specifiche registrazioni allo scopo di porre sotto controllo: (i) l'identificazione delle leggi e delle normative applicabili alle attività della Società; (ii) il monitoraggio periodico della conformità alla normativa applicabile;
- devono essere individuati i soggetti responsabili dell'identificazione e valutazione dell'applicabilità della normativa vigente e sono identificate le fonti di approfondimento normativo consultabili.

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, iprotocolli prevedono che:

- devono essere definite procedure, ruoli e responsabilità in merito alle fasi dell'attività di predisposizione eattuazione 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:
  - valutazione e controllo periodico dei requisiti di idoneità e professionalità del responsabile del servizio di prevenzione e protezione (c.d. "RSPP");
  - definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratoriaddetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;
  - processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza dellemodalità e della tempistica in caso di avvicendamento nel ruolo;
- deve essere garantita la presenza e l'aggiornamento dell'Organigramma della Sicurezza della Società (adesempio, con riferimento a RSPP, RLS, Medico Competente, Addetti antincendio e primo soccorso), monitorando tempestivamente ogni cambiamento intercorso e/o di progetti di cambiamento tecnologico, impiantistico, organizzativo e procedurale;
- deve essere 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;
- deve essere tenuta copia delle nomine degli attori coinvolti nel processo di valutazione dei rischi: almeno di RSPP, Medico Competente, RLS;
- deve essere segnalata tempestivamente l'eventuale assenza di una o più delle figure obbligatorie per legge;

- devono essere 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;
- devono essere 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 deve esserci 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. 81/2008 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.

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 eprotezione 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;
- devono essere individuate le consulenze e le professionalità esterne necessarie e da coinvolgere nella valutazione dei rischi e nell'adeguamento documentale, tecnico, impiantistico;
- deve essere definito, aggiornato e divulgato, attraverso il supporto del RSPP, il Documento di Valutazione dei Rischi (DVR);
- deve essere effettuata la valutazione dei rischi, elaborando il DVR. 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 esempio, documentazione tecnica, misure strumentali, esiti di sondaggi interni, etc.) devono essere chiari, completi e rappresentare in modo veritiero lo stato della Società;
- i dati e le informazioni devono essere 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 deve procedere: 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:
  - attività di routine e non routine;
  - attività di tutte le persone che hanno accesso al posto di lavoro (compresi esterni);
  - comportamento umano;

- pericoli provenienti dall'esterno;
- pericoli legati alle operazioni o creati nell'ambiente circostante;
- infrastrutture, attrezzature e materiali presenti presso il luogo di lavoro;
- modifiche apportate ai processi e/o al sistema di gestione, tra cui le modifiche temporanee, e il loroimpatto sulle operazioni, processi ed attività;
- eventuali obblighi giuridici applicabili in materia di valutazione dei rischi e di attuazione delle necessariemisure di controllo;

- è disponibile, in adempimento del D. Lgs. 81/2008, un Documento di Valutazione dei Rischi che individuai rischi operativi e 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 al controllo dei rischi ed elabora il programma di miglioramento mediante, tra l'altro:
  - l'individuazione delle fonti potenziali di pericolo presenti in tutte le fasi lavorative;
  - l'individuazione dei soggetti esposti;
  - l'individuazione dei danni effettivamente verificatisi in passato, sulla base dell'esame delle statistiche degli infortuni e delle malattie professionali;
  - 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 diprevenzione e protezione;
- in relazione ai Dispositivi di Protezione Individuale, è necessario che la Società:
  - identifichi le attività per le quali prevedere l'impiego di DPI e l'eventuale coinvolgimento dell'identificazione del MC e dell'RLS;
  - definisca i criteri di scelta dei DPI, che devono assicurare l'adeguatezza dei DPI stessi alle tipologie dirischio individuatein fasedi valutazione e la loro conformità alle normetecniche vigenti (ad esempio, marcatura CE);
  - definisca le modalità di consegna ed eventualmente di conservazione/manutenzione dei DPI;
  - 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.
- la Società ha definito un protocollo per l'accesso alle sedi e la gestione degli spostamenti in concomitanza dell'emergenza Covid-19, in particolare è stabilito che:
  - prima di accedere ai locali aziendali è obbligatorio recarsi in reception per il controllo della sicurezza edella temperatura;
  - è obbligatorio l'uso della mascherina chirurgica per tutti gli spostamenti all'interno dei locali aziendali, nelle sale riunioni e quando non è possibile mantenere la distanza di 1,5 metri;
  - è obbligatorio lavarsi le mani prima/ dopo l'ingresso in sede, ad ogni contatto con superfici/ oggetti aldi fuori della propria postazione, nonché prima dell'ingresso/ dopo l'utilizzo delle sale riunioni/d ei sistemi di videoconferenza;
  - è consentita la presenza concomitante di solo due persone ai distributori automatici. è vietato l'uso deifrigoriferie dei boccioni distributori di acqua. è obbligatorio utilizzare solo bicchieri e materiale monouso e usa e getta; evitare l'uso promiscuo di bottiglie, bicchieri, piatti e posate;
  - è vietato consumare il proprio pasto all'interno delle sale mensa o sale break;

- è fatto obbligo di mantenere sempre una distanza di almeno 1,5 metri con i colleghi; sono vietati gli assembramenti sia all'interno che all'esterno dei locali aziendali;
- l'uso degli ascensori è consentito ad un massimo di due persone per volta, con obbligo di indossare la mascherina;
- è fatto obbligo di mantenere puliti i propri dispositivi e prestare molta attenzione all'igiene;
- è vietato scambiarsi tra colleghi dispositivi e cancelleria;
- è vietato lasciare materiali o oggetti personali sulle postazioni di lavoro, nelle sale break e nei serviziigienici.

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 definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addettiad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;
- il Piano Antincendio e d'Emergenza deve essere definito, aggiornato e divulgato, attraverso il supporto delRSPP;
- la cassetta di primo soccorso deve essere conforme, completa e accessibile, nonché in numero congruorispetto al numero dei lavoratori o alle dimensioni degli ambienti di lavoro;
- deve essere verificato periodicamente che il contenuto minimo della cassetta di primo soccorso, previstoper legge, sia sempre presente e disponibile;
- la gestione delle emergenze viene attuata attraverso specifici piani che prevedono:
  - l'identificazione delle situazioni che possono causare una potenziale emergenza;
  - definizione delle modalità per rispondere alle condizioni di emergenza e prevenire o mitigare le relative conseguenze negative in tema di salute e sicurezza;
  - modalità e responsabilità di gestione delle prove di emergenza, con particolare riguardo alla tipologia di emergenza (ad esempio, incendio, evacuazione, etc.);
  - 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 esitidi dette prove e delle attività di verifica e di manutenzione dei presidi predisposti;
  - l'individuazione, attraverso detti piani, di percorsi di esodo e delle modalità di attuazione, da parte del personale, delle misure di segnalazione e di gestione delle emergenze;
  - la predisposizione e manutenzione in efficienza di idonei sistemi per la lotta agli incendi scelti per tipologia e numero in ragione della specifica valutazione del rischio di incendio ovvero delle indicazionifornite dall'autorità competente; sono altresì presenti e mantenuti in efficienza idonei presidi sanitari;
  - è assicurata all'interno degli spazi operativi un'adeguata organizzazione delle attività produttive al fine di consentire la corretta esecuzione delle procedure di emergenza.

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

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

- devono essere individuati i requisiti e le competenze specifiche per la conduzione delle attività di audit sulmodello di Salute e Sicurezza dei lavoratori nonché le modalità e le tempistiche delle verifiche sullo statodi 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 Società;
- deve essere assicurato l'aggiornamento della documentazione della 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 (ad esempio, verifica impianti messa a terra, impianti antincendio);
- devono essere definite le modalità di registrazione delle manutenzioni effettuate e le relative responsabilità;
- devono essere 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 devono essere 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 al processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza delle modalitàe 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 della 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 medico coordinatore l'elenco complessivo e aggiornato dei lavoratori, ogni qualvoltavi sia una nuova assunzione nonché ogni semestre, 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;
- devono essere 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 qualsiasimansione 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 protocolliprevedono che:

- devono essere 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 deve provvedere a monitorare le esigenze formative attraverso uno scadenziario con le schederelative a ciascun lavoratore;
- gli attestati e certificazioni di formazione del personale sono archiviati;
- la Società deve formare e addestrare un numero sufficiente di addetti antincendio e primo soccorso, presidiando le periodicità formative e la necessità di rinnovo;
- è necessario verificare che i consulenti esterni nominati (quali RSPP, Medico Competente) siano inpossesso degli attestati previsti per legge;
- è opportuno affidarsi – nell'organizzazione dei corsi – ad Enti o Società di consulenza abilitate ad erogare formazione valida ai sensi di legge.

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 disicurezza 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 protettiveindividuate;
- la Società ha identificato un Rappresentante dei Lavoratori per la Sicurezza, che viene consultatirelativamente alla Valutazione dei Rischi;
- la Società deve svolgere la riunione periodica ai sensi dell'art. 35 del D. Lgs. 81/2008;
- deve essere garantita la verbalizzazione della riunione annuale, quale occasione per monitorare lo stato dei rischi e di avanzamento delle misure di miglioramento e conservare il verbale sottoscritto da tutti i partecipanti;
- devono essere previste specifiche modalità che regolamentano il coinvolgimento e la consultazione deilavoratori, in particolare:
  - la comunicazione interna tra i vari livelli e funzioni dell'organizzazione;
  - la comunicazione con i fornitori ed altri visitatori presenti sul luogo di lavoro;
  - il ricevimento e alle comunicazioni dalle parti esterne interessate;
  - la partecipazione dei lavoratori, anche a mezzo delle proprie rappresentanze, attraverso:
  - il loro coinvolgimento nell'identificazione dei pericoli, valutazione dei rischi e definizione delle misure ditutela;
  - il loro coinvolgimento nelle indagini relative ad un incidente;
  - 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 definiti i ruoli, le responsabilità e le modalità di rilevazione, tracciabilità/registrazione e investigazione interna degli infortuni, incidenti occorsi e "near miss";
- devono essere definite le modalità di comunicazione da parte dei responsabili operativi al Datore di Lavoroe al responsabile del servizio di prevenzione e protezione sugli infortuni/incidenti occorsi;
- devono essere definiti i ruoli, le responsabilità e le modalità di monitoraggio degli infortuni occorsi (tenendoconto di eventuali controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro) al finedi 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 i fornitori incaricati di prestazioni di servizio, e presidiare l'andamento dei lavori relativamente ai rischi d'interferenza;
- devono essere incluse nei contratti le clausole e le verifiche richieste in materia di salute e sicurezza per le attività di approvvigionamento e gestione degli appalti;
- le attrezzature, i macchinari e gli impianti devono garantire la conformità a quanto previsto dalla normativavigente (ad esempio, marcatura CE, possesso di dichiarazione di conformità rilasciata dall'installatore, etc.);
- nel caso di acquisti di servizi, anche di natura intellettuale (ad esempio, acquisto di servizi di progettazioneda rendersi a favore della Società o di eventuali clienti), la Società:
  - 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 esempio, iscrizione ad albi professionali);
  - attua il controllo dell'operato dei fornitori attraverso le modalità previste dalle proprie procedure interne;
- devono essere 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 deve dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di RegolaritàContributiva;
- l'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi rilascia la dichiarazione diconformità alle regole dell'arte;
- deve essere tenuta copia della verifica di idoneità tecnica professionale della ditta esterna appaltatrice;
- devono essere valutate le più opportune modalità di intervento (tempi e modi) affinché sia azzerato o ridotto al minimo il rischio di interferenze lavorative. In quest'ultimo caso coordinare l'elaborazione del DUVRI – documento unico di valutazione rischi d'interferenza;
- devono essere interrotti i lavori della ditta esterna qualora questi creino pregiudizio alla salute e sicurezzadel personale aziendale, o danno ai beni aziendali;
- deve essere posta vigilanza sulle attività della ditta esterna senza interferire nell'esecuzione dei lavori propri della ditta esterna;
- devono essere segnalate immediatamente eventuali problematiche ed anomalie riscontrate durante l'esecuzione dei lavori;
- è necessario sincerarsi che la ditta esterna, al termine dei lavori, abbia ripristinato i locali, le attrezzature e gli impianti, affinché questi non creino pericoli e rischi aggiuntivi al personale aziendale (ovvero diversi da quelli valutati nel DVR).

Area di rischio: Gestione della Salute e Sicurezza sul Lavoro

Attività sensibili	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	Esempi di reato
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 circal'attuazione delle procedure di emergenza.
Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio etc.).						✓										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 esempio, 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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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. In particolare:

- TeamSystem promuove politiche produttive che contemperino le esigenze di sviluppo economico e di creazione di valore, proprie delle attività di impresa, con le esigenze di rispetto e salvaguardia dell'ambiente;
- TeamSystem in particolare, ritiene di primaria importanza la tutela dell'ambiente e lo sviluppo sostenibile del territorio in cui opera, in considerazione dei diritti della comunità e delle generazioni future;
- la Società si impegna a considerare, nell'ambito della gestione operativa e delle iniziative di business, le imprescindibili esigenze ambientali e a minimizzare l'impatto negativo che le proprie attività aziendali hanno sull'ambiente.

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 costantemente oggetto di valutazione le leggi e le norme ambientali emanate e devono essere presidiate quelle in pubblicazione;
- devono essere definite e divulgate linee guida e principi di standardizzazione degli approcci e della gestione degli impatti ambientali;

- devono essere identificate, qualora necessario, le strutture di supporto esterno (studi di consulenza, laboratori di analisi, ditte trasporto e smaltimento rifiuti, etc.) nella gestione degli aspetti cogenti e autorizzativi;
- 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 essereverificata: 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'impiantodi smaltimento e d) il metodo di trattamento o recupero;
- i rifiuti prodotti devono essere correttamente caratterizzati, classificati e identificati;
- le aree dedicate al deposito temporaneo dei rifiuti sono individuate e allestite in conformità alla normativa vigente;
- deve essere prevista la differenziazione dei rifiuti al fine di prevenire ogni illecita miscelazione;
- ciascun rifiuto deve essere chiaramente identificato mediante apposizione all'esterno del relativo contenitore di descrizione e codice identificativo;
- deve essere verificata la disponibilità e la corretta archiviazione della documentazione relativa alla gestione dei rifiuti;
- il personale deve essere informato sulle disposizioni vigenti nel territorio comunale riguardanti la raccolta differenziata e separazione tra diverse tipologie di rifiuti;
- deve essere assicurata negli ambienti di lavoro la presenza e l'uso corretto dei contenitori differenziati perla raccolta differenziata conformemente alle disposizioni degli Enti locali competenti e di controllo;
- deve essere assicurato il conferimento differenziato nei punti di raccolta esterni ai luoghi di lavoro;
- deve essere garantita la raccolta separata dei rifiuti speciali per tipologie di rifiuto;
- è necessario inviare i rifiuti a recupero/ smaltimento attraverso ditte di trasporto autorizzate al ritiro delle singole tipologie di rifiuto, assicurandosi che il trasporto/ritiro avvenga con compilazione e rilascio del FIR(Formulario di Identificazione dei Rifiuti);
- deve essere determinata per iscritto – in fase di affidamento dei lavori a ditta esterna – le responsabilità erelativi oneri di smaltimento rifiuti generati dalle attività;
- deve essere determinata per iscritto, in fase di affidamento dell'appalto, le responsabilità e relativi oneri dirimozione dei rifiuti generati dagli interventi di ristrutturazione;
- è fatto espresso divieto di:
  - compiere azioni o tenere comportamenti che siano o possano essere interpretati come pratiche voltea danneggiare la salute delle persone e/o le componenti naturali dell'ambiente;
  - conferire l'attività di gestione dei rifiuti a soggetti non dotati di un'apposita autorizzazione per il loro smaltimento e recupero;
  - violare gli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la gestione deirifiuti;
  - utilizzare impianti e apparecchiature in violazione delle disposizioni normative in materia di sostanzeozono lesive.

Area di rischio: Gestione adempimenti ambientali.

Attività sensibili	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	Esempi di reato
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, etc.).

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, tra cui svolgimento di incontri con prospect;
- Gestione delle informazioni e comunicazioni al mercato, anche attraverso il sito internet della Società;
- Gestione di sponsorizzazioni, omaggi e di altre liberalità.

Reati applicabili

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

- delitti di criminalità organizzata (art. 24-ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25);
- 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).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, che costituiscono parte integrantedello 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 conformialla 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 Anticorruzione, TeamSystem proibisce ogni forma di corruzione a favore diqualsiasi soggetto.

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.

Protocolli specifici di prevenzione

a) Attività di marketing, tra cui svolgimento di incontri con prospect.

Per l'attività sensibile attività di marketing, tra cui svolgimento di incontri con prospect, i protocolli prevedonoche:

- devono essere adottati strumenti ai fini del monitoraggio delle scadenze dei diritti di utilizzo;

- tutte le attività di comunicazioni relative alla Società devono essere preventivamente autorizzate;
- prima di condividere notizie attinenti all'attività di TeamSystem, il dipendente deve assicurarsi che le stessenon siano riservate e che provengano da fonti interne autorizzate;
- non è consentita la condivisione di materiale (ad esempio, audio o video) qualora vi sia la possibilità che tale materiale violi il diritto di autore altrui;
- la Società ha descritto nella normativa interna il processo operativo che la Società ha adottato al fine di assicurare che la documentazione fornita alla clientela rispetti le Disposizioni di Vigilanza;
- tutte le evidenze del processo di contrattualizzazione devono essere archiviate nelle apposite cartelle informatiche o fisiche, in modo che sia sempre possibile attestare che il processo definito sia stato rispettato;
- per l'attività di promozione e distribuzione dei servizi offerti, la Società si avvale prevalentemente di tecniche di comunicazione a distanza e di campagne di marketing sul territorio condotte da personale dedicato.

b) Gestione delle informazioni e comunicazioni al mercato, anche attraverso il sito internet della Società.

Per l'attività sensibile di gestione delle informazioni e comunicazioni al mercato, anche attraverso il sito internet della Società., i protocolli prevedono che:

- le informazioni acquisite dai dipendenti e/o consulenti nello svolgimento delle mansioni assegnate devonorimanere strettamente riservate e non devono essere diffuse all'interno e all'esterno dell'azienda se non nel rispetto della normativa vigente;
- il Gruppo TeamSystem considera la diffusione di informazioni corrette, complete e veritiere su tutti i fatti aziendali – ed il mantenimento della dovuta riservatezza sugli stessi, quando necessario – qualepresupposto per creare e conservare un rapporto di trasparenza e di fiducia con i propri portatori di interessi correlati e del mercato;
- l'obbligo di riservatezza si estende, oltre che alle informazioni che riguardano la Società, anche a quelle relative a clienti, fornitori, partner commerciali o agli altri soggetti con i quali si intrattengono rapporti commerciali o comunque qualificati. Conseguentemente, nella gestione delle informazioni, i dipendenti devono conservare scrupolosamente e con il massimo riserbo tutte le informazioni aziendali di qualunquetipologia apprese nell'esercizio delle proprie funzioni;
- devono essere definiti i ruoli e i compiti delle Aree/ Funzioni e dei Responsabili coinvolti nella predisposizione e divulgazione di dati e notizie all'esterno;
- il soggetto responsabile dell'emissione dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni;
- le informazioni rilevanti comunicate internamente mediante posta elettronica devono essere protette da eventuali rischi di diffusione impropria;
- devono essere individuati i soggetti cui compete il controllo sulla correttezza e divulgazione delleinformazioni e dei soggetti espressamente autorizzati alla diffusione all'esterno di dette notizie;
- devono essere individuate le Aree/ Funzioni aziendali che possono essere chiamate a intrattenere irapporti con il mercato/ la comunità finanziaria;
- è fatto espresso divieto di:
  - diffondere l'informazione rilevante all'interno o all'esterno della Società, se non tramite il canale istituzionalmente previsto;
  - diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo;
- la Società ha definito un iter operativo e ruoli e responsabilità relative ai criteri di classificazione delle informazioni aziendali;
- la gestione delle informazioni deve avvenire nel rispetto di quanto stabilito nella normativa interna a ciò predisposta;
- il proprietario delle informazioni è tenuto a: (i) classificare e gestire le informazioni aziendali di sua competenza secondo i criteri riportati nel presente documento; (ii) stabilire, ove richiesto dal livello di classifica, la lista dei

destinatari in accordo a quanto stabilito nel presente documento;(iii) aggiornare nel tempo, se necessario, il livello di classificazione da attribuire all'informazione;

- i destinatari delle informazioni sono tenuti a: (i) trattare l'informazione in loro possesso per le sole finalità e con le modalità connesse alle proprie responsabilità e mansioni lavorative e in conformità ai requisiti di sicurezza previsti per il livello di classificazione ad essa assegnata nel rispetto delle politiche e delle procedure di sicurezza aziendali e delle normative cogenti; (ii) segnalare tempestivamente ogni eventualediffusione non autorizzata o utilizzo non corretto delle informazioni classificate;
- tutte le informazioni sia cartacee che elettroniche, in qualsiasi contesto, su qualsiasi tipo di supporto e conqualsiasi mezzo esse siano conservate o comunicate, devono essere classificate in relazione al loro livellodi riservatezza;
- una informazione confidenziale può essere divulgata ad un elenco limitato e predefinito di personale interno all'Organizzazione e ai Clienti che hanno un sottoscritto un contratto per la fornitura di un servizio o un NDA (Non Disclosure Agreement);
- una informazione ad uso interno può essere divulgata a tutto il personale interno all'Organizzazione e alleterze parti che hanno in corso un rapporto di lavoro o fornitura o hanno sottoscritto un NDA (Non Disclosure Agreement);
- tutte le informazioni provenienti dall'esterno del Gruppo e utilizzate da TeamSystem nell'ambito dell'erogazione dei propri servizi (e.g., Fatturazione Elettronica alla Pubblica Amministrazione, Conservazione Digitale) devono essere classificate con livello Confidenziale, fatto salvo differente livello di classificazione associato e segnalato dal titolare delle stesse.

c) Gestione di sponsorizzazioni, omaggi e di altre liberalità.

Per l'attività sensibile di Gestione di sponsorizzazioni, omaggi e di altre liberalità, i protocolli prevedono che:

- le attività di sponsorizzazione possono riguardare i temi sociali, dell'ambiente, dello sport, dello spettacolo,dell'arte e della cultura. In ogni caso nella scelta delle proposte cui aderire la Società presta particolare attenzione a ogni possibile conflitto d'interesse di ordine personale o aziendale.
- nel corso della trattativa d'affari o rapporto commerciale sia con la Pubblica Amministrazione che con clienti e fornitori, occorre applicare criteri generali di correttezza, trasparenza e integrità. In particolare, non devono essere:
  - esaminate o proposte o promesse opportunità di impiego e/o commerciali che possano avvantaggiaredipendenti della Pubblica Amministrazione o clienti/ fornitori a titolo personale;
  - offerti in alcun modo omaggi, dazioni, benefici anche indiretti, beni, servizi e prestazioni o favori nondovuti o che travalichino gli ordinari rapporti di cortesia;
  - sollecitate o ottenute informazioni riservate che possano compromettere l'integrità o la reputazione dientrambe le parti, nonché arrecare benefici diretti o indiretti rilevanti per sé o per la Società;
  - intraprese azioni volte a influenzare impropriamente le decisioni della controparte;
- i dirigenti, i dipendenti o i collaboratori di TeamSystem non devono accettare alcun bene o servizio, regalo,beneficio, prestazione o dazione che travalichi gli ordinari rapporti di cortesia;
- il dipendente, che riceve doni o trattamenti di favore che travalichino gli ordinari rapporti di cortesia, deve darne immediatamente notizia al proprio Responsabile ovvero all'Organismo di Vigilanza;
- TeamSystem esprime un principio generale di "tolleranza zero" nella lotta alla corruzione, stabilendo cheè proibitoil ricorso a qualsiasi formadi pagamento illecito, in denaro o altra utilità (tutto ciò che rappresentaun vantaggio per la persona, materiale o morale, patrimoniale o non patrimoniale, ritenuto rilevante dalla consuetudine e dal convincimento comune), allo scopo di trarre un vantaggio nelle relazioni con i propri stakeholder. Vantaggi inteso anche come facilitazione, o garanzia del conseguimento, di prestazioni comunque dovute. TeamSystem non consente di corrispondere, offrire o accettare, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni comunque giàdovute da parte di soggetti suoi interlocutori.
- le sponsorizzazioni, affinché possano essere effettuate, devono rientrare nella sfera delle iniziative che abbiano l'esclusivo scopo di promozione istituzionale del brand, creazione di visibilità e reputazione positiva per TeamSystem;
- i partner con cui la Società intende sottoscrivere contratti di sponsorizzazione devono essere oggetto di una preventiva valutazione sulla affidabilità e sulla reputazione dell'ente;

- tutte le attività di sponsorizzazione, al fine di evitare che possano essere considerate una forma dissimulata di conferimento di un beneficio ad una terza parte per ottenere un vantaggio per la Società, devono essere contrattualizzate in forma scritta, definendo, in particolare, la natura e la finalità dell'iniziativa, nonché il corrispettivo previsto (che dovrà avere caratteristiche di congruità ed effettività rispetto alla prestazione resa);
- il soggetto beneficiario deve impegnarsi a rispettare le prescrizioni del presente Codice e delle Leggi Anticorruzione vigenti, accettando che il contratto possa essere risolto in caso di violazione delle stesse;
- gli omaggi, vantaggi economici o altre utilità, possono essere effettuati o ricevuti qualora rientrino nel contesto di atti di cortesia commerciale e siano tali da non compromettere l'integrità e/o la reputazione di una delle parti e tali da non poter essere interpretati come finalizzati a creare un obbligo di gratitudine o ad acquisire vantaggi in modo improprio;
- gli omaggi devono rispondere alle finalità di migliorare e promuovere l'immagine della Società ed a mantenere le relazioni commerciali e/o istituzionali;
- TeamSystem vieta l'effettuazione e l'accettazione, diretta o indiretta, di qualsiasi forma di regalia rivolta all'ottenimento di un improprio vantaggio, personale o di business, o che anche possa essere interpretato come tale;
- gli atti di cortesia commerciale sono consentiti solo se conformi alle procedure aziendali definite;
- regali e/o omaggi non devono essere elargiti se questo può comportare la violazione del divieto di corruzione previsto dal Codice Anticorruzione o delle relative normative di riferimento;
- le uniche forme di regalie ammesse, quale forma di cortesia commerciale, devono essere:
  - di modesto valore, ovvero commisurate alle circostanze e alla natura del destinatario;
  - concesse in buona fede e secondo il buon costume;
  - conformi agli standard di cortesia professionale generalmente accettati (ad esempio, pacco di Natale) o aventi scopi promozionali/dimostrativi;
  - non effettuate in forma di pagamento in contanti;
  - in linea con le Leggi Anticorruzione, le leggi locali e i regolamenti applicabili;
- tutti i contributi di beneficenza devono essere approvati, ai fini del rispetto delle Leggi Anticorruzione, in coerenza con le previsioni aziendali interne;
- il Responsabile della Area/ funzione interessata ad erogare l'omaggio deve farne richiesta scritta (anche via e-mail) al Responsabile competente, che effettuate le proprie verifiche, autorizza l'erogazione dell'omaggio;
- deve esistere un'autorizzazione formalizzata a conferire utilità;
- devono esistere documenti giustificativi delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità;
- gli eventuali fornitori delle utilità devono essere scelti all'interno di una lista gestita dalla Area/Funzione competente. L'inserimento / eliminazione dei fornitori dalla lista deve essere basato su criteri oggettivi. L'individuazione, all'interno della lista, del fornitore della singola utilità deve essere motivata e documentata;
- è prevista la rilevazione di operazioni (sponsorizzazioni, omaggi e liberalità) ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette;
- 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 D. Lgs. 231/2001;
- sono immediatamente interrotte o, comunque, non è data esecuzione ad operazioni relative a 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;
- devono esistere report periodici sulle spese per la concessione di utilità, con motivazioni e nominativi dei beneficiari, inviati al livello gerarchico superiore e archiviati;
- non è possibile 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 è possibile effettuare o promettere, in favore dei clienti, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito;
- nessuna 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 Anticorruzione e il Modello Organizzativo ex D. Lgs. 231/2001;
- l'inizio della prestazione deve sempre essere preceduto 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 Area/ Funzione competente autorizza l'erogazione dell'omaggio. Qualora la spesa per l'omaggio non sia stata prevista nel budget della Are/ Funzione interessata, la richiesta dovrà essere autorizzata dall'Amministratore Delegato della Società;
- la sottoscrizione del contratto deve avvenire da parte del soggetto a ciò delegato sulla base delle procure interne;
- 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 donazioni devono essere pagate in modo trasparente e tracciabile;
- 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 Anticorruzione;
- 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 (a des. 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 atti vari; 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;
- le donazioni devono essere autorizzate dal Consiglio di Amministrazione;
- il pagamento delle donazioni/ liberalità deve essere effettuato tramite bonifico o altro mezzo idoneo a consentire la tracciabilità e l'identificazione degli effettivi destinatari del contributo erogato;
- le sponsorizzazioni devono essere giustificate da uno scopo commerciale legittimo e concreto ed essere specificamente dirette all'attuazione di una strategia comunicativa commerciale;
- le sponsorizzazioni possono essere intraprese solo se il corrispettivo / contributo offerto dalla società del Gruppo TeamSystem è atteso essere proporzionale alla ragionevole aspettativa di ritorno in termini di risonanza sul pubblico di riferimento, o di ritorno di apprezzamento per il brand;
- le sponsorizzazioni non possono essere guidate da motivazioni di ordine politico;
- le sponsorizzazioni non possono essere dirette a sostenere individui privati;

- 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;
- il pagamento della sponsorizzazione deve essere effettuato tramite bonifico o altro mezzo idoneo a consentire la tracciabilità e l'identificazione degli effettivi destinatari del corrispettivo / contributo erogato;
- deve essere verificato e documentato (attraverso foto, gadget, video, etc.) l'avvenuta esecuzione della prestazione concordata durante l'evento sponsorizzato;
- deve essere previsto che la certificazione delle prestazioni erogate possa essere rilasciata dalle aree compenti sulla base della documentazione che ne attesti l'avvenuta erogazione /totale e/o parziale che deve essere messa a disposizione dell'Area Amministrazione, Finanza e Controllo per i controlli di competenza;
- deve essere previsto che la certificazione delle prestazioni erogate per importi superiori a quanto previsto contrattualmente possa essere effettuata solo in presenza di modifiche contrattuali valide;
- il contratto di sponsorizzazione o ogni altro tipo di accordo/documentazione atta a documentare la sponsorizzazione e la rispondenza ai principi elencati, la documentazione di avvenuta prestazione dovranno essere archiviate a cura dell'ente richiedente.

Area di rischio: Attività promozionali, marketing e relazioni con il mercato

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Attività di marketing, tra cui svolgimento di incontri con prospect.											✔					DA - La Società utilizza immagini tutelate da diritto d'autore senza averne acquisito i diritti di utilizzo.

Gestione delle informazioni privilegiate e comunicazioni al mercato, anche attraverso il sito internet della Società.		✔													SOC/CP - Diffusione di notizie non veritiere, ma dotate di particolare credibilità, in ordine ad importanti operazioni economiche effettuate dalla Società o da una società del Gruppo, in modo da condizionare il prezzo di uno strumento finanziario non quotato.
Gestione di 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. TRIB - Personale della società registra documentazione fittizia relativa a contributi non effettivamente concordati ed erogati alla clientela al fine di contabilizzare fraudolentemente costi inesistenti ed evadere le imposte sui redditi o sul valore aggiunto.

SEZIONE N – Gestione degli adempimenti per la prevenzione del riciclaggio e del finanziamento del terrorismo

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 degli adempimenti previsti dalla normativa antiriciclaggio e contro il finanziamento del terrorismo: (i) adeguata verifica della clientela (controlli di I e II livello); (ii) monitoraggio black-list (ad esempio, world-check); (iii) invio segnalazioni S.AR.A alla UIF; (iv) invio di segnalazioni di operazioni sospette (SOS).

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione degli adempimenti previsti dalla normativa antiriciclaggio e contro il finanziamento del terrorismo, si configurano potenzialmente le seguenti fattispecie di reato:

- delitti di criminalità organizzata (art. 24-ter);
- reati societari (art. 25-ter);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater);
- delitti contro il patrimonio culturale (25-septiesdecies);
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (25-duodeviecies).

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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 Anticorruzione TeamSystem proibisce ogni forma di corruzione a favore di qualsiasi soggetto.

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 di gestione degli adempimenti in materia antiriciclaggio e prevenzione del finanziamento del terrorismo. In particolare:

- la Società richiede massima trasparenza nelle operazioni commerciali e nei rapporti con i terzi, nel pieno rispetto delle normative, nazionali e internazionali, in tema di lotta al fenomeno del riciclaggio;
- i Destinatari del Modello non possono di conseguenza avviare rapporti d'affari per conto della Società con partner o fornitori o terzi che non diano adeguate garanzie di onorabilità e non godano di buona reputazione ovvero il cui nome sia associato a vicende connesse ad attività di riciclaggio;
- tutte le transazioni finanziarie devono trovare adeguata giustificazione nei rapporti contrattuali e devono essere effettuate mediante mezzi di pagamento che ne garantiscano la tracciabilità;
- la Società dovrà intrattenere rapporti d'affari esclusivamente con clienti e fornitori di sicura reputazione, che svolgono attività commerciali lecite e i cui proventi derivano da fonti legittime. Ciascuna unità aziendale dovrà dotarsi di misure idonee a garantire che non siano accettate forme di pagamento identificate quale strumento di riciclaggio di denaro illecito. La Società è impegnata al pieno rispetto di tutte le leggi antiriciclaggio vigenti a livello

internazionale, comprese quelle che prescrivono la denuncia di transazioni sospette in denaro contante o di altra natura.

- In ogni caso, è fatto espresso divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

  - instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
  - eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio, con il finanziamento del terrorismo;
  - ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
  - sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
  - partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;
  - mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi, risorse finanziarie o disponibilità economiche che risultino strumentali al perseguimento di attività illecite.

Protocolli specifici di prevenzione

a) Gestione degli adempimenti previsti dalla normativa antiriciclaggio e contro il finanziamento del terrorismo.

Per l'attività sensibile Gestione degli adempimenti previsti dalla normativa antiriciclaggio e contro il finanziamento del terrorismo, adeguata verifica della clientela (controlli di I e II livello), monitoraggio black-list (ad esempio, world-check), invio segnalazioni S.AR.A alla UIF, invio di segnalazioni di operazioni sospette (SOS), i protocolli prevedono che:

- deve essere effettuato il monitoraggio nel medio-lungo periodo da parte delle Strutture operative preposte che garantisca un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento (con particolare riguardo all'operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell'operazione, i fondi impiegati, il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
- devono essere adottati sistemi di controllo informatici atti ad impedire l'operatività riguardanti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi);
- la Società non instaura rapporti continuativi ovvero esegue operazioni con società bancarie di comodo (c.d. Shell Banks), cioè banche che non hanno una presenza fisica nel paese in cui sono legalmente costituite e autorizzate all'esercizio dell'attività, né sono affiliate a un gruppo finanziario soggetto a un'efficace vigilanza su base consolidata;
- la Società deve istituire adeguati presidi organizzativi e procedurali al fine di prevenire e impedire la realizzazione di operazioni di riciclaggio e di finanziamento al terrorismo. Inoltre, deve assicurarsi che nella struttura organizzativa siano rispettate le norme a tutela della prevenzione del riciclaggio e del finanziamento del terrorismo;
- in aderenza all'approccio basato sul rischio, la Società ha definito i presidi organizzativi e di controllo per la prevenzione del riciclaggio e del finanziamento del terrorismo alla luce delle caratteristiche del servizio offerto e del segmento di clientela business cui esso è destinato;
- la Società è tenuta a seguire l'iter procedurale per corretto adempimento degli obblighi in materia di antiriciclaggio e antiterrorismo, che prevede l'adeguata verifica della clientela nonché un monitoraggio costante della relazione per gli ambiti di propria competenza;

- laddove la Società si trovi nell'impossibilità oggettiva di effettuare l'adeguata verifica della clientela, la stessa si astiene dall'instaurare, eseguire ovvero proseguire il rapporto e le operazioni procedendo, se del caso, all'estinzione del rapporto continuativo già in essere e valutando se effettuare una segnalazione di operazione sospetta alla UIF.;
- la Società si astiene dall'instaurare rapporti o eseguire operazioni e pone fine al rapporto continuativo già in essere con: clienti o potenziali clienti residenti in paesi esteri (clientela non in target) e operazioni con paesi esteri cd. "ad alto rischio". In tali casi, il sistema prevede dei blocchi automatici;
- è prevista la segregazione dei compiti nelle situazioni individuate dalle disposizioni di legge e dalla normativa interna che impongono obblighi rafforzati di adeguata verifica della clientela, subordinazione dell'apertura di nuovi rapporti, del mantenimento di rapporti preesistenti e dell'esecuzione delle operazioni al rilascio di una autorizzazione da parte di una Struttura diversa da quella operativa;
- in relazione alle attività di monitoraggio dell'operatività volte ad individuare operazioni potenzialmente sospette, predisporre una segregazione in base alla quale:
  - le Aree aziendali competenti monitorano le operazioni di loro competenza, segnalando i movimenti anomali al Responsabile per la segnalazione delle operazioni sospette per gli opportuni approfondimenti e/o segnalazioni;
  - il Responsabile per la segnalazione delle operazioni sospette effettua l'analisi della segnalazione e svolge autonomamente le necessarie indagini sull'operazione sospetta, disponendo l'inoltro o meno delle segnalazioni alla competente Autorità;
- nell'ambito di una puntuale profilatura della clientela, verifica secondo un approccio risk based, all'atto dell'accensione del rapporto, da parte del Responsabile dell'Area/ Funzione competente, della correttezza e completezza dei dati censiti in anagrafe, nonché in merito alle informazioni acquisite in relazione alla attività economica svolta; tali informazioni devono essere aggiornate periodicamente rispetto al livello di rischio dei clienti mediante la riproposizione di un nuovo questionario di adeguata verifica, nonché laddove si ritengano non più attuali le informazioni acquisite in precedenza;
- è necessario verificare l'eventuale presenza del nominativo nelle versioni aggiornate delle liste specifiche "Black list" nella fase di apertura del rapporto continuativo e in occasione del monitoraggio periodico, anche avvalendosi di applicativi specialistici;
- la presenza di un soggetto all'interno delle liste sopraindicate comporta: l'immediata segnalazione al Responsabile antiriciclaggio; la tempestiva Segnalazione di Operazione Sospetta; la chiusura del rapporto;
- monitoraggio e presidio da parte delle Aree/ Funzioni preposte al controllo interno della puntuale esecuzione delle attività delle Aree operative in merito alla:
  - acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
  - valutazione delle operazioni rilevate dalle procedure informatiche in uso;
  - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
  - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;
  - registrazione dei rapporti e delle operazioni in AUI e conservazione dei documenti e delle informazioni;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Area di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto, in particolare in relazione ai rapporti continuativi e alle operazioni occasionali che rientrano nella propria attività istituzionale, la Società conserva: i dati e le informazioni acquisite tramite l'adeguata verifica della clientela; gli aggiornamenti alla documentazione stessa acquisiti in corso di rapporto; ogni altro dato o informazione che ritiene utile ai fini della normativa antiriciclaggio; "copia" di tutti i dati, le informazioni e i documenti, acquisiti in sede di instaurazione del rapporto continuativo con il cliente e per tutta la durata del rapporto; qualora fossero rilevati elementi di anomalia meritevoli di approfondimento, tali ulteriori documenti ed informazioni verranno conservate nella apposita cartella relativa al cliente;
- ai fini dell'obbligo di conservazione, la Società provvede alla conservazione dei dati e delle informazioni acquisite in sede di adeguata verifica della clientela o di controllo costante mediante inserimento degli stessi nell'AUI, mentre tutte le informazioni e i dati acquisiti mediante l'adeguata verifica della clientela, TeamSystem Payments vengono conservare nell'archivio digitale di Trust Technologies e in altro archivio digitale;

- sono adottate misure informatiche e fisiche per garantire la riservatezza delle informazioni, con particolare riguardo a quelle relative all'individuazione dei titolari effettivi e alla profilatura dei clienti;
- la documentazione raccolta a supporto delle verifiche e dei controlli che precedono la decisione di dar corso o meno alla segnalazione di operazione sospetta viene custodita con la massima riservatezza sotto la diretta responsabilità del Responsabile delle SOS;
- tutte le valutazioni e la documentazione che il Responsabile Operations trasmette al Responsabile AML e questi al Responsabile SOS, sono conservate in apposite cartelle, accessibili solo alle funzioni interessate attraverso specifiche credenziali di accesso;
- la Società ha messo in atto tutta una serie di procedure che garantiscano la riservatezza ed il divieto di comunicazione nei confronti di soggetti terzi e non solo del cliente. In particolare, la procedura di segnalazione garantisce la massima riservatezza dell'identità del soggetto segnalante;
- a seguito delle segnalazioni SOS, l'Autorità (UIF, Guardia di Finanza e DIA) può richiedere degli approfondimenti sul contenuto delle stesse. In tali casi, ricevuta la richiesta da parte della Autorità, il Responsabile SOS, con il supporto della Funzione AML, provvede a raccogliere la documentazione richiesta dall'Autorità ed a trasmetterla a mezzo PEC, nei termini previsti. La relativa richiesta ricevuta e la documentazione trasmessa vengono conservate e archiviate in apposite cartelle da parte del Responsabile SOS;
- la Società ha definito un iter operativo e ruoli e responsabilità per l'invio delle S.AR.A. In particolare, il Referente S.AR.A. provvede alla archiviazione e conservazione in modalità informatica della documentazione inerente alla segnalazione aggregata inviata;
- è prevista l'erogazione sistematica di attività specificamente dedicate alla formazione continua dei dipendenti e dei collaboratori sui profili di rischio legati alla normativa antiriciclaggio e di contrasto al finanziamento del terrorismo.
- la Società ha definito un iter operativo e ruoli e responsabilità relativi alla gestione dell'on boarding della clientela.

Area di rischio: Gestione degli adempimenti previsti dalla normativa antiriciclaggio e contro il finanziamento del terrorismo

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	RCB	
Gestione degli adempimenti previsti dalla normativa antiriciclaggio e contro il finanziamento del terrorismo: - adeguata verifica della clientela (controlli di I e II livello) - monitoraggio black-list (ad esempio, world-check) - invio segnalazioni S.AR.A alla UIF		✔	✔				✔								✔	SOC - La Società espone alle Autorità Pubbliche di Vigilanza (UIF), nelle comunicazioni periodiche previste dalle vigenti disposizioni normative in materia di Antiriciclaggio, fatti materiali non rispondenti al vero, ostacolando così l'esercizio delle funzioni di vigilanza nell'interesse o vantaggio della Società RIC - La Società omette di eseguire le segnalazioni di operazioni sospette alle Autorità competenti

- invio di segnalazioni di operazioni sospette (SOS)															(UIF) agevolando la condotta criminosa di un proprio cliente, al fine di mantenere/non perdere opportunità di business CRI - La Società non si astiene dall'intrattenere rapporti con soggetti legati alla criminalità organizzata per fini commerciali TERR - La Società non effettua i dovuti controlli sul nominativo di un cliente sulle black-list antiterrorismo ovvero classifica un match rilevante come "falso positivo" per fini Commerciali RIC BEN CUL - un soggetto apicale o sottoposto della Società agevoli un cliente (operante nel mondo dell'arte) nell'attività di reimmissione nel circuito legale di denaro o altri beni di provenienza illecita per il tramite di servizi di pagamento offerti dalla Società, non adempiendo agli obblighi antiriciclaggio.

SEZIONE O – Gestione dei rapporti con soggetti ai quali sono attribuite attività di 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 dei rapporti con soggetti ai quali sono attribuite attività di controllo, ed in particolare alle attività sensibili:

- Rapporti con gli organi di controllo (ad esempio, Collegio Sindacale, etc.) relativamente allo svolgimento dei propri compiti di vigilanza per garantire la sana e prudente gestione della Società, nonché allo svolgimento di verifiche sulla gestione amministrativa/contabile, compresa la custodia e tenuta dei libri contabili e sociali.

Reati applicabili

In relazione alle attività sensibili relative all'area di rischio gestione dei rapporti con soggetti ai quali sono attribuite attività di controllo di cui al paragrafo precedente, si configurano potenzialmente le seguenti fattispecie di reato:

- 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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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. In particolare, è previsto che nello svolgimento delle attività di verifica e controllo da parte del Collegio Sindacale, dei Revisori e dei Soci è necessario agire con trasparenza e prestare la massima collaborazione.

Protocolli specifici di prevenzione

a) Rapporti con gli organi di controllo (ad esempio, Collegio Sindacale, etc.) relativamente allo svolgimento dei propri compiti di vigilanza per garantire la sana e prudente gestione della Società, nonché allo svolgimento di 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 (ad esempio, Collegio Sindacale, etc.) relativamente allo svolgimento dei propri compiti di vigilanza per garantire la sana e prudente gestione della Società, nonché allo svolgimento di 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;
- gli OdV delle varie Società del Gruppo garantiscono 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;
- è fatto divieto di 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;
- i rapporti con il Collegio Sindacale e la Società di Revisione, sono intrattenuti dal Responsabile dell'Area di riferimento o dai soggetti dal medesimo appositamente incaricati;
- deve essere prevista la partecipazione regolare e continua del Collegio Sindacale alle riunioni del Consiglio di Amministrazione, a garanzia della effettiva conoscenza da parte del Collegio Sindacale in merito alle scelte di gestione della Società;
- deve essere prevista la tempestiva e completa evasione delle richieste di documentazione specifica avanzate dal Collegio Sindacale - anche per il tramite di terzi - nell'espletamento della propria attività di vigilanza e controllo;
- deve essere prevista la tempestiva e completa trasmissione, a cura delle strutture competenti, delle richieste di documentazione specifica avanzate dalla Società di Revisione nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili: ciascuna Area ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori;
- deve essere prevista la tempestiva e completa messa a disposizione della Società di Revisione, da parte delle strutture interessate, della documentazione disponibile relativa alle attività di controllo ed ai processi operativi seguiti, sui quali i revisori effettuano le proprie attività di verifica;
- deve essere garantita la sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo del Collegio Sindacale;
- per ciascuna Area/ 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;
- tutta la documentazione prodotta nell'ambito delle attività svolte con riferimento alla gestione dei rapporti con la Pubblica Amministrazione, delle risorse umane, dell'approvvigionamento di beni e servizi, della registrazione e qualifica dei fornitori, della tesoreria e dei flussi finanziari, delle operazioni M&A e dei rimborsi spese/trasferte, comprese eventuali comunicazioni via mail, è conservata a cura dei diversi responsabili di Area/ Funzione coinvolti nell'operazione di approvvigionamento di beni e/o servizi e messa a disposizione, su richiesta, del Presidente, del Collegio Sindacale, della Società di Revisione e dell'Organismo di Vigilanza;
- eventuali aspetti di approfondimento emersi in sede di discussione da parte del Consiglio di Amministrazione e/o eventuali successive richieste di chiarimento, provenienti dalla Società di Revisione e/o dal Collegio Sindacale, sono analizzate dal Responsabile dell'Area Amministrazione, Finanza e Controllo che fornisce le risposte/chiarimenti in tempi congrui a consentire l'emissione da parte degli organi di controllo delle rispettive relazioni nei termini di legge;
- il Responsabile della Funzione Compliance riferisce, con periodicità almeno semestrale, i risultati della propria attività al Consiglio di Amministrazione, all'Amministratore Delegato e al Collegio Sindacale della Società, attraverso relazioni riassuntive delle verifiche svolte;
- il Responsabile della Funzione Risk Management relaziona al Consiglio di Amministrazione e al Collegio Sindacale semestralmente sulle attività condotte dalla Funzione.

Area di rischio: Gestione dei rapporti con soggetti ai quali sono attribuite attività di controllo.

Attività sensibili	Categorie di reato														Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione dei rapporti con soggetti ai quali sono attribuite attività di controllo.		✔														SOC/CP - Il personale della Società effettua comunicazioni non veritiere o incomplete a fronte di richieste di informazioni da parte dei soci o del Collegio Sindacale, ovvero falsità nella consegna di documentazione relativa a procure o ad atti societari.

SEZIONE P – Gestione degli adempimenti fiscali

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 degli adempimenti fiscali., ed in particolare alle attività sensibili:

- Gestione degli adempimenti fiscali con riferimento al calcolo dell'obbligazione tributaria e alla predisposizione delle relative dichiarazioni.

Reati applicabili

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

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

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, etc.) redatti in conformità ai requisiti indicati dal D. Lgs. 231/2001, 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.

Protocolli specifici di prevenzione

a) Gestione degli adempimenti fiscali con riferimento al calcolo dell'obbligazione tributaria e alla predisposizione delle relative dichiarazioni.

Per l'attività sensibile gestione degli adempimenti fiscali con riferimento al calcolo dell'obbligazione tributaria e alla predisposizione delle relative dichiarazioni, i protocolli prevedono che:

- la Società è tenuta a rispettare i termini e le modalità previsti dalla normativa applicabile per la predisposizione delle dichiarazioni annuali e per i conseguenti versamenti relativi alle imposte sui redditi e sul valore aggiunto;
- è fatto divieto di esibire documenti negligentemente incompleti e/o comunicare dati falsi o alterati ad Enti Pubblici;
- è fatto divieto di indicare elementi attivi per un ammontare superiore/inferiore a quello effettivo o elementi passivi fittizi (ad esempio, costi fittiziamente sostenuti e/o ricavi indicati in misura superiore/inferiore a quella reale), avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti, anche tramite una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;

- deve essere previsto un piano che assicuri la formazione nel continuo del personale dell'Area Amministrazione, Finanza e Controllo e che ne garantisca l'aggiornamento normativo;
- deve essere prevista l'analisi degli andamenti (ad esempio, liquidazione IVA periodica in linea con andamenti acquisti di periodo). Eventuali variazioni anomale e le principali variazioni intercorse rispetto al periodo precedente sono indagate e verificate;
- deve essere prevista la verifica della corrispondenza tra gli importi contabilizzati e quelli utilizzati per la determinazione delle imposte;
- l'Area Amministrazione, Finanza e Controllo, in sede di determinazione del fondo imposte, effettua controlli circa l'inerenza fiscale dei costi contabilizzati analizzando i conti ritenuti più significativi (o per importo o per la natura dei costi imputati);
- devono essere effettuate riconciliazioni dei conti fiscali e controlli sulle poste indetraibili /indeducibili;
- devono essere svolte valutazioni relative alle variazioni in aumento / in diminuzione;
- deve essere previsto che siano effettuate valutazioni relative alle perdite pregresse e alle imposte anticipate e differite;
- deve essere stabilito un processo per l'approvazione interna del primo calcolo imposte prima dell'invio al consulente fiscale;
- il fiscalista esterno deve effettuare la revisione delle componenti di reddito non deducibili e non detraibili;
- il fiscalista esterno deve verificare il calcolo delle imposte rispetto alla vigente normativa (TUIR, normativa nazionale e locale, giurisprudenza tributaria, etc.);
- deve essere stabilito che, in seguito alle verifiche del fiscalista esterno, vi sia l'approvazione formale della bozza di dichiarazione da parte dell'Area Amministrazione, Finanza e Controllo prima della firma del legale rappresentante (in funzione delle vigenti procure);
- deve essere stabilito che sia sottoposta a processi di archiviazione la documentazione a supporto della dichiarazione pre e post la presentazione della stessa;
- la Società, ai fini della determinazione delle imposte dirette e indirette, correnti e differite, deve predisporre adeguata documentazione di supporto dalla quale si evinca la completezza e l'accuratezza dei calcoli sottostanti la determinazione delle imposte;
- la Società ha definito un iter operativo e ruoli e responsabilità relative alla gestione degli adempimenti fiscali e, più in particolare, al calcolo delle imposte di competenza;
- la Società ha definito i documenti necessari al rispetto da parte della Area Amministrazione, Finanza e Controllo degli obblighi fiscali e normativi ai fini della gestione delle scadenze fiscali e normative annuali;
- tutti i documenti e le informazioni necessari al rispetto da parte della Area Amministrazione, Finanza e Controllo degli obblighi fiscali e normativi ai fini della gestione delle scadenze fiscali e normative annuali devono essere predisposti e adeguatamente archiviati.

Area di rischio: Gestione degli adempimenti fiscali.

Attività sensibili	Categorie di reato															Esempi di reato
	PA	SOC/C	RIC	IT	IND*	SSL	CRI	AMB	IMP	MA	DA	PI	FA	TSN	TRIB	
Gestione degli adempimenti fiscali con riferimento al calcolo dell'obbligazione tributaria e alla predisposizione delle relative dichiarazioni.			✔				✔							✔	✔	RIC - La Società investe i proventi derivanti dalla evasione fiscale, perpetrata tramite la predisposizione di dichiarazioni fraudolente, nell'ambito della propria attività economica. CRI/TSN - Tre o più persone all'interno della Società si associano al fine di commettere un reato rilevante. TRIB - La Società presenta una dichiarazione con elementi rivenienti da fatture per operazioni inesistenti, previamente registrate, con le quali si costituiscono elementi passivi fittizi o attivi inferiori a quelli reali.