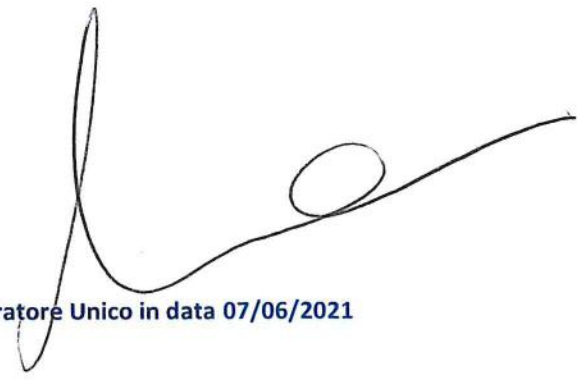
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

in attuazione del Decreto legislativo 8 giugno 2001, n. 231

IT.CITY S.p.A. a socio unico



Approvato con determina dell'Amministratore Unico in data 07/06/2021

INDICE

STRUTTURA DEL DOCUMENTO 6

PARTE GENERALE 7

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 7
1.1 Introduzione 7
1.2 Fattispecie di reato contemplate dal Decreto 7
1.3 I presupposti della responsabilità amministrativa dell'ente 8
1.4 La natura della responsabilità dell'ente e relative sanzioni 10
1.5 Le vicende modificative dell'ente 11
1.6 L'esenzione dalla responsabilità: caratteristiche del Modello 11
1.7 Le Linee Guida elaborate dalle associazioni di categoria 12
1.8 Evoluzione giurisprudenziale 13
1.9 Legge 190/2012 13
1.10 Decreto Legislativo 33/2013 14

2. LA SOCIETÀ E IL SUO SISTEMA DI GOVERNANCE ORGANIZZATIVA 14
2.1 Sistema di Governance 14
2.2 Direzione 15

3. L'ADOZIONE DEL MODELLO 17
3.1 Finalità del Modello 17
3.2 Approvazione del Modello e nomina degli Organismi di Controllo 17
3.2 Codice Etico 18
3.3 Attività propedeutiche svolte per la realizzazione del Modello 18
3.4 Modalità di aggiornamento del Modello 19
3.5 Reati rilevanti per la Società 19
3.6 Destinatari del Modello 20

4. ORGANISMI DI CONTROLLO 20
4.1 Il D. Lgs. 231/2001 e l'istituzione dell'Organismo di Vigilanza 20
4.2 Legge 190/2012 e l'istituzione del Responsabile della Prevenzione della Corruzione 22
4.3 Il D. Lgs. 33/2013 e l'istituzione del Responsabile della Trasparenza 23
4.4 Flussi informativi nei confronti degli Organismi di Controllo 24
4.5 Gestione delle segnalazioni verso gli Organismi di Controllo 24
4.6 Flussi informativi dagli Organismi di controllo al top management 25
4.7 Il coordinamento con le direzioni aziendali 25
4.8 Le risorse dell'Organismo di Vigilanza 25

5. IL SISTEMA DISCIPLINARE 26
5.1 Sistema disciplinare 26
5.2 Destinatari 26
5.3 Criteri di applicazione delle sanzioni 27
5.4 Misure per i dipendenti 27
5.5 Misure per i dirigenti 29
5.6 Misure nei confronti di lavoratori autonomi 29
5.7 Misure nei confronti degli amministratori 29

6. COMUNICAZIONE E FORMAZIONE 30
6.1 Piano di comunicazione interna 30
6.2 Piano di comunicazione esterna 30
6.3 Piano di formazione 30

PARTE SPECIALE 31

1. Introduzione 31
2. Principi generali di comportamento 31
3. Protocolli generali di prevenzione 31
4. Attività strumentali alla commissione di reati e protocolli specifici di prevenzione 32

SEZIONE A **36**
REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E REATI DI CORRUZIONE **36**
A.1 Premessa 36
A.2 Fattispecie incriminatrici applicabili 37
A.3 Attività sensibili 39
A.4 Principi generali di comportamento 39
A.5 Protocolli specifici di prevenzione 40
SEZIONE B **44**
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI **44**
B.1 Fattispecie incriminatrici applicabili 44
B.2 Attività sensibili 45
B.3 Protocolli generali di prevenzione 45
B.4 Protocolli specifici di prevenzione 46
B.5 Delitti informatici e Codice della Privacy 48
SEZIONE C **50**
DELITTI DI CRIMINALITÀ ORGANIZZATA E REATI TRASNAZIONALI **50**
C.1 Fattispecie incriminatrici applicabili 50
C.2 Attività sensibili 51
C.3 Protocolli specifici di prevenzione 51
SEZIONE D **52**
DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO **52**
D.1 Fattispecie incriminatrici applicabili 52
D.2 Attività sensibili 52
D.3 Protocolli specifici di prevenzione 52
SEZIONE E **53**
REATI SOCIETARI E CORRUZIONE TRA PRIVATI **53**
E.1 Fattispecie incriminatrici applicabili 53
E.2 Attività sensibili 54
E.3 Protocolli specifici di prevenzione 54
SEZIONE F **56**
REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME PER VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI SALUTE E SICUREZZA DEI LUOGHI DI LAVORO **56**
F.1 Premessa 56
F.2 Attività sensibili 57
F.2.1 Premessa 57
F.2.2 Le attività sensibili 58
F.3 Principi generali di comportamento 59
F.4 Protocolli specifici di prevenzione 59
F.5 Ulteriori controlli 64
F.6 Attività di audit per la verifica periodica dell'applicazione e dell'efficacia delle procedure 66
SEZIONE G **67**
REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO **67**
G.1 Fattispecie incriminatrici applicabili 67
G.2 Premessa: il reato di autoriciclaggio 67
G.3 Attività sensibili 68
G.4 Protocolli specifici di prevenzione 68
SEZIONE H **70**
DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE **70**
H.1 Fattispecie incriminatrici applicabili 70
H.2 Attività sensibili 72
H.3 Protocolli generali di prevenzione 72
H.4 Protocolli specifici di prevenzione 72
H.5 Attività sensibili affidate, in tutto o in parte, a soggetti terzi 73
SEZIONE I **74**
INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA **74**
I.1 Fattispecie incriminatrice applicabile 74
I.2 Attività sensibili e prevenzione 74
SEZIONE J **75**
REATI AMBIENTALI **75**
J.1 Fattispecie incriminatrici applicabili 75
J.2 Attività sensibili 75
J.3 Protocolli generali di prevenzione 75

J.4 Protocolli specifici di prevenzione 76
SEZIONE K **78**
IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE **78**
K.1 Fattispecie incriminatrice applicabile 78
K.2 Attività sensibili 78
K.3 Protocolli specifici di prevenzione 78
SEZIONE L **78**
REATI TRIBUTARI **78**
K.1 Fattispecie incriminatrice applicabile 78
K.2 Attività sensibili 78
K.3 Protocolli specifici di prevenzione 78

Allegato 1: Dichiarazione di responsabilità e di assenza di conflitti di interesse **79**

Allegato 2: Dichiarazione e clausola risolutiva da inserire negli incarichi a collaboratori e consulenti esterni **80**

Allegato 3: Dichiarazione e clausola risolutiva da inserire negli incarichi a fornitori **81**

Revisioni			
N.	**Data**	**Descrizione**	**Riferimenti**
01	28.04.2014	Prima redazione del documento	
02	03.06.2014	Documento modificato per approvazione	
03	24.06.2014	Documento Approvato con DAU n° 20 2014	Prot. 2014-218
04	11.02.2015	Aggiornamento estensione dei reati previsti dalla Legge 190/2012 e gli adempimenti previsti dalla legge 33/2013	
05	31.01.2017	Aggiornamento estensione dei reati pr<evisti dagli artt. 24, 25, 24-bis, 24-ter, 25-bis.1, 25-septies, 25-octies, 25-novies, 25-decies, 25-undecies, 25-duodecies del D. Lgs. 231/2001 e dell'art. 10 L. 146/2006.	
06	31.03.2020	Aggiornamento estensione dei reati previsti dall'art. 25 *quinquiesdecies* inserito dall'art. 39, comma 2, del D.L. 26.10.2019, n. 124, convertito in legge dalla L. 19.12.2019, n. 157.	
07	01.06.2021	Aggiornamento estensione dei reati previsti dal Dlgs 14 luglio n.75 recante 'Attuazione della direttiva Europea 2017/1371' c.d. direttiva PIF per quanto applicabili alle attività della Società.	Prot. 2021/197/PG

GLOSSARIO

SOCIETÀ O IT.CITY S.P.A	IT.CITY S.p.A. a socio unico con sede legale in Largo Torello De Strada, 11/a, 43121 Parma PR
DECRETO	Decreto Legislativo 8 giugno 2001, n. 231[1].
REATI PRESUPPOSTO	gli specifici reati individuati dal Decreto da cui può derivare la responsabilità amministrativa dell'ente, nonché, per quanto ad essi assimilabili, gli specifici illeciti amministrativi in relazione ai quali è prevista l'applicazione delle norme contenute nello stesso Decreto.
ATTIVITÀ SENSIBILI	attività della Società nel cui ambito sussiste il rischio, anche potenziale, di commissione di reati di cui al Decreto
GRUPPO COMUNE DI PARMA	le Società controllate dal Comune di Parma soggette ad attività di direzione e coordinamento da parte del Comune.
MODELLO	il presente documento composto dall'insieme di disposizioni e di protocolli attraverso i quali viene definita la struttura aziendale, i processi di gestione e l'ambito di controllo finalizzati a garantire i principi di correttezza e trasparenza nello svolgimento delle attività aziendali, nonché a prevenire la commissione di reati in cui vi sia la responsabilità amministrativa di IT City.
DESTINATARI DEL MODELLO	tutti i soggetti tenuti al rispetto delle prescrizioni del Modello o dei relativi protocolli di attuazione
SOGGETTI APICALI	persone che rivestono funzioni di rappresentanza, 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 o il controllo della SOCIETÀ[2]
SOGGETTI SUBORDINATI	persone sottoposte alla direzione o alla vigilanza dei soggetti di cui al punto precedente
DIPENDENTI	Tutti i soggetti 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[3]
PARTNER	le controparti contrattuali della Società, persone fisiche o giuridiche, con cui la stessa addivenga ad una qualunque forma di collaborazione contrattualmente regolata
CONSULENTI	soggetti che, in ragione delle competenze professionali, prestano la propria opera intellettuale in favore o per conto della Società sulla base di un mandato o di altro rapporto di collaborazione professionale
ORGANISMO DI VIGILANZA - ODV	l'organismo previsto dall'art 6 del Decreto, preposto alla vigilanza sul funzionamento e sull'osservanza del modello organizzativo ed al relativo aggiornamento
COLLABORATORI	soggetti che intrattengono con la SOCIETÀ rapporti di collaborazione senza vincolo di subordinazione; i rapporti di agenzia; di rappresentanza commerciale ed altri rapporti che si concretino in una prestazione professionale, non a carattere subordinato, sia continuativa sia occasionale.
LINEE GUIDA DI CONFINDUSTRIA	documento-guida di Confindustria (approvato il 7 marzo 2002 ed aggiornato al marzo 2014) per la costruzione dei modelli di organizzazione, gestione e controllo di cui al Decreto

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

[2] Art. 5.1, lett. a) del DECRETO.

[3] Si intendono compresi i rapporti di lavoro di collaborazione coordinata e continuativa, a progetto, per le fattispecie escluse dall'applicazione degli art. 61 e ss. d. lgs. 276 del 2003.

STRUTTURA DEL DOCUMENTO

Il presente documento è composto da una **Parte Generale** e una **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, le modalità di funzionamento degli Organismo di Controllo, la definizione di un sistema disciplinare 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 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 *control & risk self assessment* finalizzato all'individuazione delle attività sensibili, qui integralmente richiamato e agli atti della Società;
- il *Codice Etico*, che definisce i principi e le norme di comportamento della Società;
- *Piano Triennale di Prevenzione della Corruzione e della Trasparenza*;
- gli *Strumenti di attuazione del Modello;*

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

PARTE GENERALE

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

1.1 Introduzione

In data 8 giugno 2001 è stato emanato - in esecuzione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300 - il Decreto legislativo n. 231 (di seguito denominato il "**Decreto**"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia ha già da tempo aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

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

La natura di questa nuova forma di responsabilità degli enti è di genere "misto" e la sua peculiarità risiede nel fatto che la stessa coniuga aspetti del sistema sanzionatorio penale e di quello amministrativo. In base al Decreto, infatti l'ente è punito con una sanzione di natura amministrativa, in quanto risponde di un illecito amministrativo, ma il sistema sanzionatorio è fondato sul processo penale: l'Autorità competente a contestare l'illecito è il pubblico ministero, ed è il giudice penale che irroga la sanzione.

La responsabilità amministrativa dell'ente è distinta ed autonoma rispetto a quella della persona fisica che commette il reato e sussiste anche qualora non sia stato identificato l'autore del reato, o quando il reato si sia estinto per una causa diversa dall'amnistia. In ogni caso, la responsabilità dell'ente va sempre ad aggiungersi, e mai a sostituirsi, a quella della persona fisica autrice del reato.

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

1.2 Fattispecie di reato contemplate dal Decreto

L'ente può essere chiamato a rispondere soltanto per i reati, cc.dd. reati presupposto, indicati dal Decreto o comunque da una legge che preveda espressamente la responsabilità amministrativa dell'ente e le relative sanzioni ed entrata in vigore prima della commissione del fatto di reato.
Alla data di approvazione del presente documento, i reati presupposto appartengono alle categorie indicate di seguito:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- delitti informatici e trattamento illecito di dati (art. 24-*bis*);
- delitti di criminalità organizzata (art. 24-*ter*);
- reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis*)
- delitti contro l'industria e il commercio (art. 25-*bis.1*);
- reati societari, inclusa la *corruzione tra privati* (art. 25-*ter*);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater*);
- pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1);

- delitti contro la personalità individuale, inclusi l'intermediazione illecita e lo sfruttamento del lavoro di cui all'art. 603-*bis* c.p. , per come introdotti dalla legge n. 199 del 2016 (art. 25-*quinquies*);
- abusi di mercato (art. 25-*sexies*);
- reati transnazionali (art. 10 legge n. 146 del 16 marzo 2006);
- reati di omicidio colposo e lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies*);
- reati di 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*).

L'elenco dei reati sopra indicati è suscettibile di modifiche ed integrazioni da parte del legislatore. Da qui l'esigenza di una costante verifica sull'adeguatezza di quel sistema di regole che costituisce il modello di organizzazione, gestione e controllo, previsto dal Decreto e funzionale alla prevenzione dei reati.

La rilevanza di ciascun reato per la Società e la conseguente applicabilità della previsione che lo contempla sono oggetto di approfondimento al paragrafo 3.5 "Reati rilevanti per la Società".

1.3 I presupposti della responsabilità amministrativa dell'ente

I presupposti della responsabilità dell'ente sono indicati nell'art. 5 del Decreto:

"L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

a) 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 dello stesso;
b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi".

Oltre alla commissione di uno dei reati presupposto, affinché l'ente sia sanzionabile ai sensi del D.Lgs. 231/2001 devono essere integrati altri requisiti normativi. Tali ulteriori criteri di imputazione della responsabilità agli enti possono essere distinti in "oggettivi" e "soggettivi".

Il primo criterio oggettivo è integrato dal fatto che il reato sia stato commesso da parte di un soggetto legato all'ente da un rapporto qualificato. In proposito si distingue tra:

- soggetti in "posizione apicale", cioè che rivestono posizioni di rappresentanza, amministrazione o direzione dell'ente, quali, ad esempio, il legale rappresentante, l'amministratore, il direttore di un'unità organizzativa autonoma, nonché le persone che gestiscono, anche soltanto di fatto, l'ente stesso. Si tratta delle persone che effettivamente hanno un potere autonomo di prendere decisioni in nome e per conto dell'ente. Sono inoltre assimilabili a questa categoria tutti i soggetti delegati dagli amministratori ad esercitare attività di gestione o direzione dell'ente o di sue sedi distaccate;
- soggetti "subordinati", ovvero tutti coloro che sono sottoposti alla direzione ed alla vigilanza dei soggetti apicali. Appartengono a questa categoria i Dipendenti e i Collaboratori e quei soggetti che, pur non facendo parte del personale, hanno una mansione da compiere sotto la direzione ed il controllo di soggetti apicali. Tra i soggetti esterni interessati, oltre ai Collaboratori, vi sono anche i promotori e i Consulenti, che su mandato dell'ente compiono attività in suo nome. Rilevanti sono, infine, anche i mandati o i rapporti

contrattuali con soggetti non appartenenti al personale dell'ente, sempre nel caso in cui questi soggetti agiscano in nome, per conto o nell'interesse dell'ente stesso.

Ulteriore criterio oggettivo è che il reato dovrà infine essere commesso nell'interesse o a vantaggio dell'ente. I due requisiti sono cumulabili, ma è sufficiente uno solo per delineare la responsabilità dell'ente.

L'"interesse" sussiste quando l'autore del reato ha agito con l'intento di favorire l'ente, indipendentemente dalla circostanza che poi tale obiettivo sia stato realmente conseguito.

Il "vantaggio" sussiste quando l'ente ha tratto – o avrebbe potuto trarre – dal reato un risultato positivo, economico o di altra natura.

Secondo la Corte di Cassazione (Cass. Pen., 20 dicembre 2005, n. 3615), i concetti di interesse e vantaggio non vanno intesi come concetto unitario, ma dissociati, essendo palese la distinzione tra quello che potrebbe essere inteso come un possibile guadagno prefigurato come conseguenza dell'illecito, rispetto ad un vantaggio chiaramente conseguito grazie all'esito del reato. In tal senso si è pronunciato anche il Tribunale di Milano (ord. 20 dicembre 2004), secondo cui è sufficiente la sola finalizzazione della condotta criminosa al perseguimento di una data utilità, a prescindere dal fatto che questa sia effettivamente conseguita.

La responsabilità dell'ente sussiste non soltanto quando esso ha tratto un vantaggio patrimoniale immediato dalla commissione del reato, ma anche nell'ipotesi in cui, pur nell'assenza di tale risultato, il fatto trovi motivazione nell'interesse dell'ente. Il miglioramento della propria posizione sul mercato o l'occultamento di una situazione di crisi finanziaria, ad es., sono casi che coinvolgono gli interessi dell'ente senza apportargli però un immediato vantaggio economico. È importante inoltre evidenziare che, qualora il reato venga commesso da soggetti qualificati di un ente appartenente ad un gruppo, il concetto di interesse può essere esteso in senso sfavorevole alla società capogruppo. Il Tribunale di Milano (ord. 20 dicembre 2004) ha sancito che l'elemento caratterizzante l'interesse di gruppo sta nel fatto che questo non si configura come proprio ed esclusivo di uno dei membri del gruppo, ma come comune a tutti i soggetti che ne fanno parte. Per questo motivo si afferma che l'illecito commesso dalla controllata possa essere addebitato anche alla controllante, purché la persona fisica che ha commesso il reato – anche a titolo di concorso – appartenga anche funzionalmente alla stessa.

Quanto ai criteri soggettivi di imputazione del reato all'ente, questi attengono agli strumenti preventivi di cui lo stesso si è dotato al fine di prevenire la commissione di uno dei reati previsti dal Decreto nell'esercizio dell'attività di impresa. Il Decreto, infatti, per il caso di reati commessi da soggetti apicali, prevede l'esonero da responsabilità dell'ente solo se lo stesso dimostri:

- che l'organo dirigente 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;
- che il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- che le persone hanno commesso il reato eludendo fraudolentemente il modello di organizzazione e di gestione;
- che non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di vigilanza.

Le condizioni appena elencate devono concorrere congiuntamente affinché la responsabilità dell'ente possa essere esclusa.

Nonostante il modello funga da causa di non punibilità sia che il reato presupposto sia stato commesso da un soggetto in posizione apicale, sia che sia stato commesso da un soggetto in posizione subordinata, il meccanismo previsto dal Decreto in tema di onere della prova è molto più severo per l'ente nel caso in cui il reato sia stato commesso da un soggetto in posizione apicale. In quest'ultimo caso, infatti, l'ente deve dimostrare altresì che le persone hanno commesso il reato eludendo fraudolentemente il modello e che non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza; il Decreto richiede quindi una prova di estraneità più forte, in quanto l'ente deve anche provare una condotta fraudolenta da parte dei soggetti apicali.
Nell'ipotesi di reati commessi da soggetti in posizione subordinata, l'ente può invece essere chiamato a rispondere solo qualora si accerti che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza, comunque esclusa se, prima della commissione del reato, l'ente si è dotato di un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello commesso. Si tratta, in questo

caso, di una vera e propria colpa in organizzazione: l'ente ha acconsentito indirettamente alla commissione del reato, non presidiando le attività né i comportamenti dei soggetti a rischio di commissione di un reato presupposto.

1.4 La natura della responsabilità dell'ente e relative sanzioni

La natura della responsabilità introdotta dal Decreto è oggetto di discussione. Per quanto formalmente definita "amministrativa", è nella realtà una responsabilità molto vicina a quella penale.

Il sistema sanzionatorio previsto dal D.Lgs. 231/2001 è articolato in quattro tipi di sanzione, cui può essere sottoposto l'ente in caso di condanna ai sensi del Decreto:

- **sanzione pecuniaria**: è sempre applicata qualora il giudice ritenga l'ente responsabile. Essa viene calcolata tramite un sistema basato su quote, che vengono determinate dal giudice nel numero e nell'ammontare: il numero delle quote, da applicare tra un minimo e un massimo che variano a seconda della fattispecie, dipende dalla gravità del reato, dal grado di responsabilità dell'ente, dall'attività svolta per eliminare o attenuare le conseguenze del reato o per prevenire la commissione di altri illeciti; l'ammontare della singola quota va invece stabilito, tra un minimo di € 258,00 e un massimo di € 1.549,00, a seconda delle condizioni economiche e patrimoniali dell'ente;
- **sanzioni interdittive**: le sanzioni interdittive si applicano, in aggiunta alle sanzioni pecuniarie, soltanto se espressamente previste per il reato per cui l'ente viene condannato e solo nel caso in cui ricorra almeno una delle seguenti condizioni:
  - ✓ l'ente ha tratto dal reato un profitto rilevante e il reato è stato commesso da un soggetto apicale, o da un soggetto subordinato qualora la commissione del reato sia stata resa possibile da gravi carenze organizzative;
  - ✓ in caso di reiterazione degli illeciti.

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

  Eccezionalmente applicabili in via definitiva, le sanzioni interdittive sono temporanee, con una durata che varia da tre mesi a due anni, ed hanno ad oggetto la specifica attività dell'ente cui si riferisce l'illecito. Esse possono essere applicate anche in via cautelare, prima della sentenza di condanna, su richiesta del Pubblico Ministero, qualora sussistano gravi indizi della responsabilità dell'ente e fondati e specifici elementi che facciano ritenere concreto il pericolo di ulteriore commissione di illeciti della stessa indole di quello per cui si procede;
- **confisca**: con la sentenza di condanna è sempre disposta la confisca del prezzo o del profitto del reato o di beni o altre utilità di valore equivalente. Il profitto del reato è stato definito dalle Sezioni Unite della Corte di Cassazione (v. Cass. Pen., S.U., 27 marzo 2008, n. 26654) come il vantaggio economico di diretta e immediata derivazione causale dal reato, e concretamente determinato al netto dell'effettiva utilità conseguita dal danneggiato nell'ambito di un eventuale rapporto contrattuale con l'ente; le Sezioni Unite hanno inoltre specificato che da tale definizione deve escludersi qualsiasi parametro di tipo aziendalistico, per cui il profitto non può essere identificato con l'utile netto realizzato dall'ente (tranne che nel caso, normativamente previsto, di commissariamento dell'ente). Per il Tribunale di Napoli (ord. 26 luglio 2007) non può inoltre considerarsi estranea al concetto di profitto la mancata diminuzione patrimoniale determinata dal mancato esborso di somme per costi che si sarebbero dovuti sostenere;
- **pubblicazione della sentenza di condanna**: può essere disposta quando l'ente è condannato ad una sanzione interdittiva; consiste nella pubblicazione della sentenza una sola volta, per estratto o per intero,

in uno o più giornali indicati dal giudice nella sentenza nonché mediante affissione nel Comune ove l'ente ha la sede principale, ed è eseguita a spese dell'ente.

Le sanzioni amministrative a carico dell'ente si prescrivono al decorrere del quinto anno dalla data di commissione del reato.

La condanna definitiva dell'ente è iscritta nell'anagrafe nazionale delle sanzioni amministrative da reato.

1.5 Le vicende modificative dell'ente

Il Decreto disciplina il regime della responsabilità dell'ente in caso di trasformazione, fusione, scissione e cessione di azienda.

In caso di trasformazione dell'ente resta ferma la responsabilità per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto. Il nuovo ente sarà quindi destinatario delle sanzioni applicabili all'ente originario, per fatti commessi anteriormente alla trasformazione.

In caso di fusione, l'ente risultante dalla fusione stessa, anche per incorporazione, risponde dei reati dei quali erano responsabili gli enti che hanno partecipato alla fusione. Se essa è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il giudice dovrà tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

Nel caso di scissione, resta ferma la responsabilità dell'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto e gli enti beneficiari della scissione sono solidalmente obbligati al pagamento delle sanzioni pecuniarie inflitte all'ente scisso nei limiti del valore del patrimonio netto trasferito ad ogni singolo ente, salvo che si tratti di ente al quale è stato trasferito anche in parte il ramo di attività nell'ambito del quale è stato commesso il reato; le sanzioni interdittive si applicano all'ente (o agli enti) in cui sia rimasto o confluito il ramo d'attività nell'ambito del quale è stato commesso il reato. Se la scissione è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il giudice dovrà tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

In caso di cessione o di conferimento dell'azienda nell'ambito della quale è stato commesso il reato, salvo il beneficio della preventiva escussione dell'ente cedente, il cessionario è solidalmente obbligato con l'ente cedente al pagamento della sanzione pecuniaria, nei limiti del valore dell'azienda ceduta e nei limiti delle sanzioni pecuniarie che risultano dai libri contabili obbligatori o dovute per illeciti di cui il cessionario era comunque a conoscenza.

1.6 L'esenzione dalla responsabilità: caratteristiche del Modello

Il Decreto si limita a disciplinare alcuni principi generali in merito al modello di organizzazione, gestione e controllo, senza fornirne però caratteristiche specifiche.
Il modello opera quale causa di non punibilità solo se:

- efficace, ovvero se ragionevolmente idoneo a prevenire il reato o i reati del tipo di quello o quelli commesso/i;
- effettivamente attuato, ovvero se il suo contenuto trova applicazione nelle procedure aziendali e nel sistema di controllo interno.

Quanto all'efficacia del modello, il Decreto prevede che esso debba rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, siano previste misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

Inoltre, affinché sia efficacemente attuato, il Modello, relativamente alle fattispecie considerate, richiede verifiche periodiche e modifiche quando necessario in relazione a violazioni verificatesi e a mutamenti dell'organizzazione o dell'attività nonché un idoneo sistema disciplinare (artt. 6, comma 1, lettera b) e 7, comma 4). È infine previsto che negli Enti di piccole dimensioni il compito di vigilanza possa essere svolto direttamente dall'organo dirigente (art. 6, comma 4).

L'adozione di un modello preventivo è una possibilità che la legge ha introdotto, rimettendola alla scelta discrezionale dell'ente. Esso, tuttavia, è l'unico strumento che ha l'ente per svolgere un'azione di prevenzione dei reati, dimostrare la propria non colpevolezza ed evitare le sanzioni previste dal Decreto.

1.7 Le Linee Guida elaborate dalle associazioni di categoria

Le varie associazioni di categoria, in applicazione del Decreto hanno elaborato apposite Linee Guida per la costruzione del Modello. In particolare Confindustria ha approvato il testo definitivo[4] delle proprie "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001", che possono essere schematizzate secondo le seguenti fasi fondamentali:

- "identificazione dei rischi: ossia l'analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D.Lgs. n. 231/2001";

- "progettazione del sistema di controllo (c.d. protocolli per la programmazione della formazione ed attuazione delle decisioni dell'ente): ossia la valutazione del sistema esistente all'interno dell'ente ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, i rischi identificati".

È opportuno evidenziare che la difformità rispetto a punti specifici delle diverse Linee Guida non inficia di per sé la validità del Modello. Il singolo Modello infatti, dovendo essere redatto con riguardo alla realtà concreta dell'ente cui si riferisce, ben può discostarsi dalle Linee Guida che, per loro natura, hanno carattere generale.

Le componenti maggiormente rilevanti del sistema di controllo che si desumono anche dalle Linee Guida di categoria sono:

- Codice Etico;
- sistema organizzativo;
- procedure manuali e informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo di gestione;
- sistema disciplinare e meccanismi sanzionatori;
- Organismo di Vigilanza;
- comunicazione al personale e sua formazione.

Le componenti del sistema di controllo devono essere uniformate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (ad esempio, nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
    - autonomia e indipendenza;

[4] In data 7 marzo 2002, successivamente aggiornate il 31 marzo 2008 poi nell'ultima versione al marzo 2014.

- professionalità;
- continuità d'azione;
- obblighi di informazione dell'Organismo di Vigilanza.

1.8 Evoluzione giurisprudenziale

Ai fini della redazione del presente Modello, sono stati tenuti in considerazione anche gli orientamenti giurisprudenziali che si sono formati in materia.

In particolare, sebbene in un primo momento le pronunce riguardanti la responsabilità amministrativa degli enti ex D.Lgs. n. 231/2001 non siano entrate nel merito dell'adeguatezza dei sistemi di controllo, successivamente si è andata formando una giurisprudenza la quale si è occupata di verificare l'effettiva adeguatezza, le tempistiche di adozione e l'idoneità del modello, rispetto alle esigenze ed alle caratteristiche degli enti adottanti (Trib. Milano, Sez. 4 Pen. 4 febbraio 2013, n. 13976; Cass. Pen. Sez. 5, 30 gennaio 2014, n. 4677).

Nella varietà delle decisioni emergono alcuni riferimenti costanti al fine di verificare l'idoneità del Modello adottato, quali il riferimento alle condotte criminose per cui si procede, alla struttura organizzativa, alle dimensioni, al tipo di attività ed alla storia anche giudiziaria della società coinvolta nel procedimento.

Più in particolare, i Giudici hanno valutato:

(i) l'autonomia ed indipendenza in concreto dell'Organismo di Vigilanza;
(ii) l'analiticità e completezza nell'individuazione delle aree a rischio;
(iii) la previsione di specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
(iv) la previsione di obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
(v) l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate.

1.9 Legge 190/2012

La Legge 190/2012 ha innovato profondamente l'approccio al tema della corruzione, affrontandolo, oltre che dal punto di vista penalistico, anche da un punto di vista amministrativo e comportamentale, promuovendo i comportamenti rispettosi dell'etica pubblica e della trasparenza.
Tale normativa vuole avere lo scopo di favorire la realizzazione e l'applicazione di un sistema strutturato di procedure e di attività di controllo volte a prevenire il verificarsi di fenomeni corruttivi all'interno dell'Azienda.

L'applicazione della L. 190/12 nelle società partecipate da enti pubblici e negli enti di diritto privato prevede l'introduzione di specifiche prescrizioni finalizzate all'individuazione e alla prevenzione dei rischi derivanti da fenomeni corruttivi.

Sulla base delle indicazioni fornite dal Dipartimento della Funzione Pubblica nel caso in cui sia già adottato un modello di organizzazione e gestione del rischio sulla base del D. Lgs. n. 231 del 2001, l'applicazione della Legge 190/12 può fare perno su tale modello, ma dovrà prevedere l'estensione dell'ambito di applicazione a tutti quei reati considerati nella L. 190 del 2012, dal lato attivo e passivo.

La normativa prevede la redazione di un Piano Triennale di Prevenzione alla Corruzione, il cui contenuto minimo può essere ricondotto a quanto previsto anche nell'art. 6 del D.Lgs.231/01, con l'ulteriore previsione dei seguenti punti:

- previsione delle modalità di gestione delle risorse umane (oltre a quelle finanziarie);
- previsione esplicita della necessità del Codice di comportamento;
- previsione della necessità di un sistema informativo per attuare il flusso delle informazioni e consentire il monitoraggio sull'implementazione del modello da parte dell'amministrazione vigilante.

Gli enti pubblici economici e gli enti di diritto privato in controllo pubblico, di livello nazionale o regionale/locale devono, inoltre, nominare un responsabile per l'attuazione dei propri Piani di prevenzione della corruzione, che può essere individuato anche nell'organismo di vigilanza previsto dall'art. 6 del D.lgs. n. 231 del 2001".

1.10 Decreto Legislativo 33/2013

Il D. Lgs. 33/2013, in attuazione ai commi 35 e 36 dell'art. 1 della Legge 190/2012, interviene sui temi del riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.
Tale decreto introduce la trasparenza come strumento per garantire l'accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.
Ogni amministrazione deve adottare un Programma triennale per la trasparenza e l'integrità, da aggiornare annualmente, che indica le iniziative previste per garantire:

- un adeguato livello di trasparenza, anche sulla base delle linee guida elaborate dalla Commissione di cui all'articolo 13 del decreto legislativo 27 ottobre 2009, n. 150;
- la legalità e lo sviluppo della cultura dell'integrità.

Il D. Lgs. 33/2013, alla luce della novella normativa ad opera della Legge 114/2014, si applica per intero alle società controllate dalle pubbliche amministrazioni "limitatamente alle attività di pubblico interesse".

2. LA SOCIETÀ E IL SUO SISTEMA DI GOVERNANCE ORGANIZZATIVA

2.1 Sistema di Governance

L'assetto organizzativo, gestionale e di controllo (governance organizzativa) costituisce l'impatto generale sul quale si innestano le regole proprie del Modello e le azioni degli Organismi di Controllo, la cui efficacia ne è pertanto in larga parte condizionata.
Ai sensi dell'art. 2381 c.c. 5° comma, compete all'Amministratore Unico curare l'adeguatezza dell'assetto organizzativo/contabile in relazione alla natura e dimensione dell'impresa, mentre compete al Collegio Sindacale, ai sensi dell'art. 2403 c.c., valutarne sia l'adeguatezza che il concreto funzionamento. Ciò premesso:

- l'*Amministratore Unico* adempie il suo dovere di curare l'adeguatezza organizzativa attraverso la definizione e il controllo della struttura operativa, delle mansioni, dei ruoli e delle responsabilità attribuite. Gli obiettivi di efficacia aziendale (redditività e sviluppo) sono realizzati dalla società IT.CITY attraverso la massima valorizzazione delle risorse umane ed economiche in un ambiente operativo basato sull'assunzione ponderata dei rischi d'impresa, sulla responsabilità del management nella gestione dei processi di *core business*, sul controllo interno, sulla trasparenza informativa e sulla conformità a norme e regolamenti.
- il *Collegio sindacale*, oltre al monitoraggio del rispetto della legge, dello Statuto e dei principi di corretta amministrazione attuato mediante verifiche di conformità a norme, regolamenti e procedure, vigila sull'adeguatezza organizzativa e sul suo concreto funzionamento.

Il sistema dei poteri operativi della Società IT.CITY nel suo complesso è tale da configurare in linea di principio:

- un'organizzazione adeguata all'adozione delle iniziative e di tutti gli atti di gestione aventi rilevanza esterna o interna necessari al perseguimento degli obiettivi aziendali e congruente con le responsabilità assegnate al soggetto;
- un fattore di prevenzione (mediante la definizione dei limiti e la qualificazione dei poteri assegnati a ciascun soggetto) dell'abuso dei poteri funzionali attribuiti;
- un elemento di incontrovertibile riconducibilità degli atti aziendali aventi rilevanza e significatività esterna o interna alle persone fisiche che li hanno adottati.

Tale sistema, che definisce il complesso delle responsabilità spettanti agli organi delegati e a dirigenti/funzionari nel contesto dell'attività di *core business*, comporta necessariamente margini di discrezionalità propri dell'azione manageriale o comunque di un'operatività qualificata nei suoi contenuti. La discrezionalità implicita nel potere attribuito è in ogni caso tale da risultare oggettivamente circoscritta, oltre che dalle norme di riferimento e dal contenuto formale e sostanziale degli accordi con terzi, anche dal quadro complessivo di coerenza definito dalle

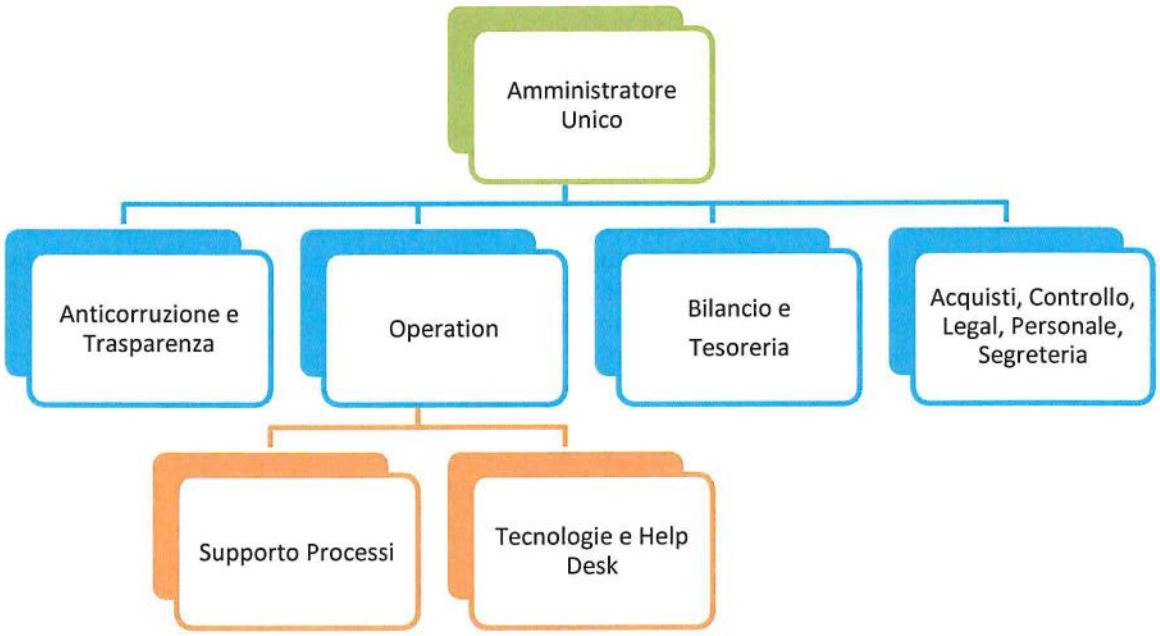
strategie, dagli obiettivi aziendali enunciati e condivisi e dalle metodologie operative consolidate nella storia aziendale nella conduzione degli affari sociali.

Nella rivisitazione organizzativa preliminare all'adozione del Modelloed al fine di collocare le prescrizioni dello stesso in un contesto di chiarezza organizzativa, si è avuto cura di verificare che:

- tutti i processi omogenei aventi rilevanza in termini gestionali sono ricondotti ad un unico responsabile di riferimento collocato formalmente in organigramma con esplicite mansioni, responsabilità e deleghe assegnate;
- l'organizzazione è tale da garantire chiarezza delle gerarchie, direzione e coordinamento, monitoraggio e rendicontazione periodica delle attività svolte;
- le deleghe e poteri, ed eventuali procure sono coerenti con le mansioni assegnate e commisurate al perseguimento degli obiettivi aziendali nei termini della corretta gestione e dell'osservanza di norme e regolamenti;
- è osservato il principio della separazione delle funzioni incompatibili;
- a ciascun dirigente e funzionario competono, oltre al coordinamento delle attività relative alla missione assegnata, la valutazione e gestione dei rischi inerenti, la misurazione delle performance, il reporting per linea gerarchica, il controllo budgetario, la valorizzazione, valutazione e supervisione del personale assegnato, la cura e salvaguardia degli assets gestiti.

2.2 Direzione

La Direzione aziendale è costituita dalle seguenti aree:



In conformità con quanto dettato dallo Statuto, l'Organo Amministrativo, costituito dall'Amministratore Unico, è investito di poteri per la gestione e l'amministrazione, sia ordinaria che straordinaria, della Società, con la limitazione a 200.000 euro per gli atti negoziali non previsti a Budget. L'Amministratore Unico ha facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione ed il raggiungimento degli scopi sociali, esclusi soltanto quelli che la legge in modo tassativo riserva all'Assemblea.

Annualmente l'Organo Amministrativo predispone il budget di esercizio ed il piano investimenti con apposita relazione da sottoporre alla preventiva autorizzazione, ai sensi dell'art. 2364 comma 5, codice civile, dell'assemblea dei soci con le modalità stabilite nel contratto di servizio.

L'organo Amministrativo può pure nominare procuratori speciali e mandatari in genere per determinati atti o categorie di atti, definendone i poteri e gli emolumenti.

Inoltre nel Regolamento del Gruppo Comune di Parma, sono definite le funzioni assegnate all'Organo Amministrativo, in particolare:

- collegamento istituzionale con il Comune;
- sorveglianza all'attività gestionale e della corretta esecuzione delle deliberazioni assembleari e di Consiglio;
- responsabile del sistema di controllo interno (c.d. audit interno).

3. L'ADOZIONE DEL MODELLO

In osservanza delle disposizioni del Decreto, la Società, con determinazione dell'Amministratore Unico del 24 giugno 2014 ha adottato il proprio Modello di organizzazione, gestione e controllo (di seguito denominato il "Modello"), successivamente aggiornato con determinazione del 31 Gennaio 2017.

L'adozione del Modello da parte della Società costituisce un modo di rafforzare e migliorare il proprio sistema di controllo interno, ed in generale la propria *corporate governance*.

3.1 Finalità del Modello

La Società IT.CITY ha elaborato ed adottato il presente Modello nella convinzione che tale strumento, oltre a realizzare la condizione esimente dalla responsabilità stabilita dalla legge, possa migliorare la sensibilità di coloro che operano per conto della Società sull'importanza di conformarsi non solo a quanto imposto dalla normativa applicabile, ma anche ai principi deontologici a cui si ispira la Società al fine di svolgere la propria attività ai massimi livelli di legittimità, correttezza e trasparenza.

In tale ottica il presente Modello trova un'applicazione più ampia del D. Lgs. 231/2001 ed è esteso anche alla prevenzione dei reati di corruzione previsti dalla Legge 190/2012 e agli obblighi di trasparenza previsti dal D. Lgs. 33/2013.

Il Modello introduce anche le figure deputate alla gestione e al controllo di quanto previsto dalle disposizione normative, che in aggiunta all'*Organismo di Vigilanza* previsto dal D. Lgs. 231/01, sono identificabili in:

- *Responsabile della Prevenzione della Corruzione*
- *Responsabile per la trasparenza*

Il Modello si propone, inoltre, le seguenti finalità:

- fornire un'adeguata informazione ai dipendenti, a coloro che agiscono su mandato della Società, o sono legati alla Società stessa da rapporti rilevanti ai fini del Decreto, con riferimento alle attività che comportano il rischio di commissione di reati;
- diffondere una cultura d'impresa che sia basata sulla legalità, in quanto la Società condanna ogni comportamento non conforme alla legge o alle disposizioni interne, ed in particolare alle disposizioni contenute nel proprio Modello;
- diffondere una cultura del controllo e di risk management;
- attuare un'efficace ed efficiente organizzazione dell'attività di impresa, ponendo l'accento in particolar modo sulla formazione delle decisioni e sulla loro trasparenza e tracciabilità, sulla responsabilizzazione delle risorse dedicate alla assunzione di tali decisioni e delle relative attuazioni, sulla previsione di controlli, preventivi e successivi, nonché sulla gestione dell'informazione interna ed esterna;
- attuare tutte le misure necessarie per ridurre il più possibile e in breve tempo il rischio di commissione di reati.

3.2 Approvazione del Modello e nomina degli Organismi di Controllo

Il presente Modello è atto di emanazione dell'Amministratore Unico. L'Amministratore Unico istituisce anche i seguenti Organismi di Controllo:

- ***Organismo di Vigilanza*** (nel seguito anche "OdV"), con il compito di vigilare sul funzionamento, sulla efficacia e sulla osservanza delle disposizioni contenute nel presente documento, nonché di curarne l'aggiornamento continuo.
- ***Responsabile della Prevenzione della Corruzione*** (nel seguito anche "RPC"), con il compito di mettere in atto le opportune attività di controllo e monitoraggio per prevenire i reati di corruzione previsti dalla Legge 190/2012.
- **Responsabile della Trasparenza** (nel seguito anche "RT"), con il compito di mettere in atto le opportune attività per la conformità con le disposizioni del D. Lgs. 33/2013.

Data la struttura organizzativa della Società si è ritenuto di optare per un OdV monocratico che durerà in carica tre anni a decorrere dalla data della nomina. La composizione dell'OdV, i suoi compiti ed i suoi poteri, vengono tempestivamente comunicati alla Società mediante pubblicazione del presente documento (es: rete intranet aziendale) o affissione in un luogo accessibile a tutti.
I membri dell'OdV sono nominati mediante uno specifico atto di nomina, reso noto attraverso gli opportuni canali.
Le nomine di *Responsabile della Prevenzione della Corruzione* e di *Responsabile della Trasparenza* sono state assegnate ad un'unica figura interna all'azienda in quanto non si ravvede un'incompatibilità degli incarichi.
Non si segnalano incompatibilità che la stessa figura ricopra un ruolo anche all'interno dell'Organismo di Vigilanza.
Le descrizioni dei requisiti, compiti, regole di funzionamento, flussi informativi da e verso gli Organismi di Controllo sono approfonditi nel capitolo 4 "L'Organismo di Vigilanza".
Nel seguito del documento ci si riferirà con il termine Organismi di Controllo per intendere singolarmente o nella pluralità OdV, RPC e RT.

3.2 Codice Etico

La Società si è dotata di un Codice Etico e del *Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT)*, il cui fine ultimo consiste nel diffondere e rendere noti ai dipendenti ed ai collaboratori i valori della Società stessa, ai quali sono tenuti ad attenersi. Onestà, integrità, rispetto delle leggi, dei regolamenti e dei codici deontologici costituiscono i valori fondanti della cultura organizzativa e dell'attività svolta dalla Società.

Il Modello presuppone il rispetto di quanto previsto nel Codice Etico e nel PTPCT, formando con essi un corpus di norme interne finalizzate alla diffusione di una cultura improntata all'etica ed alla trasparenza aziendale.

Il Codice Etico e il PTPCT della Società, in tutte le sue future riformulazioni, **si intendono qui integralmente richiamati e costituiscono il fondamento essenziale del Modello**, le cui disposizioni si integrano con quanto in esso previsti.

3.3 Attività propedeutiche svolte per la realizzazione del Modello

Il Modello di IT.CITY S.p.A è stato elaborato tenendo conto dell'attività concretamente svolta dalla Società, della sua struttura, nonché della natura e delle dimensioni della sua organizzazione. Resta peraltro inteso che il Modello verrà sottoposto agli aggiornamenti che si renderanno necessari, in base alla futura evoluzione della Società e del contesto in cui la stessa si troverà ad operare.

La Società ha proceduto ad un'analisi del proprio contesto aziendale e delle aree di attività che presentano profili potenziali di rischio, in relazione alla commissione dei reati indicati dal Decreto. In particolar modo, sono stati analizzati: il contesto societario, l'assetto organizzativo, il sistema di *corporate governance* esistente, il sistema delle procure e delle deleghe, i rapporti giuridici esistenti con soggetti terzi, la realtà operativa, le prassi e le procedure formalizzate e diffuse all'interno della Società per lo svolgimento delle operazioni.

Ai fini della preparazione del presente documento la Società ha proceduto:

- all'identificazione dei processi, sotto-processi o attività aziendali in cui è possibile che siano commessi i reati presupposto indicati nel Decreto, mediante interviste con i Responsabili delle Funzioni aziendali;
- all'autovalutazione dei rischi (c.d. *control & risk self assessment*) di commissione di reati e del sistema di controllo interno idoneo a prevenire comportamenti illeciti;
- all'identificazione di adeguati presidi di controllo, già esistenti o da implementare nelle procedure operative e prassi aziendali, necessari per la prevenzione o per la mitigazione del rischio di commissione dei reati di cui al Decreto;
- all'analisi del proprio sistema di deleghe e poteri e di attribuzione delle responsabilità.

In relazione alla possibile commissione dei reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione della normativa sulla salute e sicurezza sul lavoro (art. 25-*septies* del Decreto), la Società ha proceduto all'analisi del proprio contesto aziendale e di tutte le attività specifiche svolte, nonché alla valutazione dei rischi a ciò connessi sulla base di quanto risulta dalle verifiche svolte in ottemperanza alle previsioni del D. Lgs. 81/2008 e della normativa speciale ad esso collegata.

3.4 Modalità di aggiornamento del Modello

L'Amministratore Unico, anche grazie alle indicazioni fornite dall'Organismo di Vigilanza, delibera in merito all'aggiornamento del Modello e del suo adeguamento in relazione a modifiche e integrazioni che si dovessero rendere necessarie in conseguenza di:

- significative violazioni delle prescrizioni del Modello;
- modifiche dell'assetto interno della Società e delle modalità di svolgimento delle attività d'impresa;
- modifiche normative;
- risultanze dei controlli.

Una volta approvate, le modifiche e le istruzioni sono comunicate all'Organismo di Vigilanza, per la loro immediata applicazione fermo restando che l'Amministratore Unico provvederà, senza indugio, a rendere le stesse modifiche operative e a curare la corretta comunicazione dei contenuti all'interno e all'esterno della Società.

Rimane, in ogni caso, di esclusiva competenza dell'Amministratore Unico la delibera di aggiornamenti e di adeguamenti del Modello dovuti ai seguenti fattori:

- intervento di modifiche normative in tema di responsabilità amministrativa degli enti;
- identificazione di nuove attività sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività d'impresa;
- formulazione di osservazioni da parte del Ministero della Giustizia sulle Linee Guida a norma dell'art. 6 del Decreto e degli artt. 5 e ss. del D.M. 26 giugno 2003, n. 201;
- formulazione di osservazioni da parte dell'ANAC;
- commissione dei reati richiamati dal Decreto da parte dei Destinatari del Modello del presente documento o, più in generale, di significative violazioni del Modello;
- riscontro di carenze o lacune nelle previsioni del Modello a seguito di verifiche sull'efficacia del medesimo.

Il Modello sarà, in ogni caso, sottoposto a procedimento di revisione periodica con cadenza triennale, da disporsi mediante determina dell'Amministratore Unico.

3.5 Reati rilevanti per la Società

In considerazione della struttura e delle attività svolte dalla Società, il management coinvolto nell'analisi ha individuato come rilevanti i seguenti reati presupposto:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- delitti informatici e trattamento illecito di dati (art. 24-*bis*);
- delitti di criminalità organizzata (art. 24-*ter*);
- delitti contro l'industria e il commercio (art. 25-bis.1)
- reati societari, inclusa la corruzione tra privati (art. 25-*ter*);
- omicidio colposo o lesioni gravi o gravissime, commesse 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, inclusi gli ecoreati (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, Legge 16 Marzo 2006, n.146).

Il presente documento individua, nella successiva Parte Speciale, per ciascuna categoria di reati rilevanti per IT.CITY, le attività della Società denominate sensibili a causa del rischio insito di commissione dei reati della specie di quelli qui elencati e prevede per ciascuna delle attività sensibili principi di prevenzione e presidi dicontrollo.

La Società valuta costantemente la rilevanza ai fini del Modello di eventuali ulteriori reati, sia già previsti sia di futura previsione nel Decreto.

3.6 Destinatari del Modello

Sono destinatari del Modello:

- tutti gli amministratori e coloro che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché coloro che esercitano, anche di fatto, la gestione e il controllo della Società;
- tutti coloro che intrattengono con la Società un rapporto di lavoro subordinato (dipendenti), ivi compresi coloro che sono distaccati per lo svolgimento dell'attività;
- tutti coloro che collaborano con la Società, in forza di un rapporto di lavoro parasubordinato (collaboratori a progetto, prestatori di lavoro temporaneo, interinali, ecc.).

Il Modello si applica, altresì, a coloro i quali, pur non essendo funzionalmente legati alla Società da un rapporto di lavoro subordinato o parasubordinato, agiscano sotto la direzione o vigilanza dei vertici aziendali della Società.

L'insieme dei Destinatari così definiti è tenuto a rispettare, con la massima diligenza, le disposizioni contenute nel Modello e procedure negli strumenti di attuazione del Modello.

Il Modello viene comunicato ai Destinatari, con le modalità stabilite al successivo paragrafo 6 "Comunicazione e Formazione".

4. Organismi di Controllo

4.1 Il D. Lgs. 231/2001 e l'istituzione dell'Organismo di Vigilanza

Come noto il Decreto 231/01 ha introdotto una nuova forma di responsabilità delle persone giuridiche per alcuni tipi di reati commessi da tutti i soggetti che agiscono in nome e per conto delle stesse. Il Legislatore però, esime la Società dalla responsabilità se l'organo dirigente, oltre ad aver adottato ed attuato un idoneo modello di organizzazione, gestione e controllo, ha affidato ad un Organismo di Vigilanza il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne il suo aggiornamento (art. 6 Decreto 231/01).
La compiuta esecuzione dei propri compiti da parte dell'OdV costituisce elemento essenziale affinché la società possa usufruire dell'esimente prevista dal decreto.

4.1.1 Organismo di Vigilanza: cause di ineleggibilità e/o decadenza

I membri dell'OdV sono scelti tra soggetti qualificati ed esperti in ambito legale, aziendale e di sistemi di controllo interno.
Costituiscono cause di ineleggibilità e/o decadenza dalla carica di OdV:

- le stesse circostanze riferite agli Amministratori di cui all'art. 2382 del Codice Civile;
- la sentenza di condanna o di patteggiamento, anche non definitiva, per aver commesso uno dei reati previsti dal Decreto;
- la sentenza di condanna (o di patteggiamento) anche non definitiva a pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, oppure l'interdizione, anche temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;
- il trovarsi in situazioni che gravemente ledono l'autonomia e l'indipendenza nello svolgimento delle attività di controllo proprie dell'OdV (es. esistenza di rapporti di parentela con i membri dell'Amministratore Unico

o soggetti apicali della Società; l'esistenza di rapporti di natura patrimoniale con la Società, fatto salvo l'eventuale rapporto di lavoro subordinato, ecc..).

Qualora nel corso dell'incarico dovesse sopraggiungere una delle cause di decadenza, il membro interessato è tenuto ad informare immediatamente l'Amministratore Unico.

4.1.2 Organismo di vigilanza: i requisiti

IT.CITY attua rigorosamente le prescrizioni del Decreto in relazione ai requisiti che l'Organismo deve possedere e mantenere nel tempo. In particolare:

- l'**autonomia e l'indipendenza** sono garantiti con l'inserimento in una posizione referente all'Amministratore Unico; l'Organismo è collocato altresì in posizione referente al Collegio Sindacale per fatti censurabili che dovessero coinvolgere gli amministratori. Il requisito dell'autonomia è garantito inoltre dalla non attribuzione all'ODV di compiti operativi rilevanti ai fini 231/01 (che ne minerebbero l'obiettività di giudizio nel momento delle verifiche);
- la **professionalità** è garantita dall'esperienza dell'Organismo che è dotato delle competenze specialistiche proprie di chi svolge attività consulenziali o ispettive e necessarie per l'espletamento delle proprie funzioni. In particolare l'Organismo è dotato di:
  - competenze legali: adeguata padronanza nella interpretazione delle norme di legge con specifica preparazione nell'analisi delle fattispecie di reato individuabili nell'ambito dell'operatività aziendale e nella identificazione di possibili comportamenti sanzionabili;
  - competenze nella organizzazione: sufficiente preparazione in materia di analisi dei processi organizzativi aziendali e nella predisposizione di procedure adeguate alle dimensioni aziendali, nonché dei principi generali sulla legislazione in materia di "*compliance*" e dei controlli correlati.
  - competenze "ispettive": esperienza in materia di controlli interni maturati in ambito aziendale;
- la **continuità d'azione** è garantita dalla calendarizzazione delle attività dell'Organismo, dalla periodicità dei propri interventi ispettivi, dalla regolarità delle comunicazioni verso i vertici aziendali, come meglio decritto nello specifico regolamento di funzionamento.

4.1.3 Organismo di Vigilanza: i compiti

L'Organismo di Vigilanza ha le seguenti attribuzioni:

- vigilanza sulla effettività del Modello attraverso la verifica della coerenza tra i comportamenti concreti e quelli previsti dal Modello, mediante il presidio delle aree a rischio di reato, sia di quelle caratterizzanti l'attività tipica di IT City, sia di quelle strumentali alla commissione dei reati (gestione delle risorse finanziarie ecc).
  Per poter ottemperare a tali doveri l'Organismo di Vigilanza può stabilire attività di controllo ad ogni livello operativo, dotandosi di strumenti necessari a segnalare tempestivamente anomalie e disfunzioni del Modello, verificando ed integrando le procedure di controllo; in particolare il Modello prevede che per ogni operazione ritenuta a rischio specifico debba essere tenuta a disposizione dell'Organismo di Vigilanza un'adeguata documentazione a cura dei referenti delle singole funzioni. Ciò consentirà di procedere, in ogni momento, alla effettuazione dei controlli che descrivono le caratteristiche e le finalità dell'operazione ed individuino chi ha autorizzato, registrato e verificato l'operazione;

- verifica periodica dell'adeguatezza del Modello, cioè della capacità di prevenire i comportamenti non voluti, del mantenimento nel tempo dei requisiti di solidità e funzionalità, attraverso un monitoraggio costante sul sistema dei controlli e sui protocolli;

- aggiornamento del Modello nel caso in cui i controlli operati rendano necessari correzioni ed adeguamenti. In particolare l'Organismo di Vigilanza deve:
  - mantenere aggiornato il Modello conformemente alla evoluzione della Legge, nonché in conseguenza delle modifiche alla organizzazione interna e all'attività aziendale;
  - collaborare alla predisposizione ed integrazione della normativa interna (protocolli, procedure di controllo, ecc.) dedicata alla prevenzione dei rischi;
  - identificare, misurare e monitorare adeguatamente tutti i rischi individuati o individuabili rispetto ai reali processi e procedure aziendali procedendo ad un costante aggiornamento dell'attività di rilevazione e mappatura dei rischi;
  - promuovere iniziative atte a diffondere la conoscenza del Modello tra gli organi ed i dipendenti della Società fornendo le istruzioni ed i chiarimenti eventualmente necessari e istituendo specifici seminari di formazione;

- suggerire soluzioni organizzative e gestionali per mitigare i rischi relativi alle diverse aree esposte a rischio reato;
- provvedere a coordinarsi con le altre funzioni aziendali per un miglior controllo delle attività e per tutto quanto attenga alla concreta attuazione del Modello;
- disporre verifiche straordinarie e/o indagini mirate, con possibilità di accedere direttamente alla documentazione rilevante laddove si evidenzino disfunzioni del Modello o si sia verificata la commissione dei reati oggetto delle attività di prevenzione.

Fermo restando le disposizioni normative ed il potere discrezionale dell'OdV di attivarsi con specifici controlli di propria iniziativa o a seguito delle segnalazioni ricevute, esso effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

4.1.4 Organismo di Vigilanza: regole di funzionamento

L'attività dell'Organismo di Vigilanza è caratterizzata da un'adeguata formalizzazione con redazione di verbali idonei a documentare le attività di controllo eseguite e gli accessi effettuati in presenza del rischio di commissione di un reato presupposto o in presenza di criticità in una delle aree sensibili.
A tale scopo deve dotarsi di un regolamento che disciplini gli aspetti e le modalità principali dell'esercizio della propria azione. In particolare, devono essere disciplinati i seguenti profili:

- la tipologia delle attività di verifica e di vigilanza svolte;
- la tipologia delle attività connesse all'aggiornamento del Modello;
- l'attività connessa all'adempimento dei compiti di informazione e formazione dei destinatari del Modello;
- il funzionamento e l'organizzazione interna (ad esempio: modalità di convocazione e quorum deliberativi, verbalizzazione delle riunioni, ecc.).

Per quanto riguarda nello specifico la calendarizzazione delle riunioni, il regolamento deve prevedere che l'OdV si riunisca almeno trimestralmente, e comunque, ogni qualvolta sia necessario.

4.2 Legge 190/2012 e l'istituzione del Responsabile della Prevenzione della Corruzione

L'art. 1 comma 7 della Legge 190/2012 prevede la nomina del responsabile della prevenzione della corruzione per tutte le Pubbliche Amministrazioni. Tale previsione è stata estesa anche a tutti gli enti pubblici economici e agli enti di diritto privato in controllo pubblico, indicando la possibilità che lo stesso sia individuato anche nell'Organismo di Vigilanza ex D. Lgs. 231/2001.

La scelta del responsabile anticorruzione deve ricadere preferibilmente su dirigenti che siano titolari di ufficio di livello dirigenziale generale. Tuttavia, nelle ipotesi in cui la società sia priva di dirigenti o questi siano in numero così limitato da poter svolgere esclusivamente compiti gestionali nelle aree a rischio corruttivo, il responsabile potrà essere individuato in un funzionario che garantisca le idonee competenze. Tale soggetto non deve essere destinatario di provvedimenti giudiziali di condanna o disciplinari. Il Soggetto preposto a tale ruolo deve aver dato dimostrazione nel tempo di comportamento integerrimo.

Inoltre, nella scelta occorre tener conto quale motivo di esclusione, dell'esistenza di situazioni di conflitto di interesse evitando, per quanto possibile la designazione di dirigenti incaricati in settori considerati esposti al rischio.

4.2.1 Compiti

Il Responsabile individuato ai sensi del comma 7, entro il 31 gennaio di ogni anno, deve predisporre il Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) da sottoporre all'Amministratore Unico per l'adozione e la comunicazione al dipartimento della Pubblica Amministrazione competente.
Il responsabile, entro lo stesso termine, dovrà definire le procedure appropriate per selezionare e formare, ai sensi del comma 10, i dipendenti destinati ad operare in settori particolarmente esposti alla corruzione.
La mancata predisposizione del PTPC e la mancata adozione delle procedure per la selezione e la formazione dei dipendenti costituiscono elementi di valutazione della responsabilità dirigenziale.

Il responsabile della prevenzione della corruzione deve provvedere anche:

- alla verifica dell'efficace attuazione del piano e della sua idoneità, nonché a proporre la modifica dello stesso quando sono accertate significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività dell'amministrazione;
- alla verifica, d'intesa con il dirigente competente, dell'effettiva rotazione degli incarichi negli uffici preposti allo svolgimento delle attività nel cui ambito è più elevato il rischio che siano commessi reati di corruzione;
- all'aggiornamento del sistema di prevenzione dei rischi (es. risk assessment) in riferimento alle attività presidiate;
- suggerire soluzioni organizzative e gestionali per mitigare i rischi relativi alle diverse aree esposte a rischio reato.

4.2.2 Responsabilità

In caso di commissione, all'interno dell'amministrazione, di un reato di corruzione accertato con sentenza passata in giudicato, il responsabile della prevenzione della corruzione risponde ai sensi dell'articolo 21 del decreto legislativo 30 marzo 2001, n.165, e successive modificazioni, nonché sul piano disciplinare, oltre che per il danno erariale e all'immagine della pubblica amministrazione, salvo che provi tutte le seguenti circostanze:

- di avere predisposto, prima della commissione del fatto, il piano triennale di prevenzione della corruzione e di aver osservato le prescrizioni relative agli obblighi di formazione del personale;
- di aver vigilato sul funzionamento e sull'osservanza del piano.

4.3 Il D. Lgs. 33/2013 e l'istituzione del Responsabile della Trasparenza

L'art. 43 del D. Lgs. 33/2013 dispone che, deve essere nominato il "Responsabile per la Trasparenza" individuabile nel medesimo soggetto nominato "Responsabile per la prevenzione della corruzione".
Il Responsabile per la Trasparenza svolge stabilmente un'attività di controllo sull'adempimento degli obblighi di pubblicazione previsti dalla normativa vigente, assicurando la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate.

4.3.1 Obblighi di pubblicazione

Il D. Lgs. 33/2013 già contiene indicazioni di fonte primaria circa le modalità di pubblicazione dei documenti e delle informazioni rilevanti, nonché circa i dati da pubblicare per le varie aree di attività.
Per quanto riguarda gli enti diversi dalle pubbliche amministrazioni, il comma 34 dell'art. 1 della Legge 190/2012 prevede che gli enti pubblici economici, le società a partecipazione pubblica e le società da queste controllate ai sensi dell'art. 2359 c.c. gli enti pubblici vigilati, gli enti di diritto privato in controllo pubblico e le società partecipate (secondo le accezioni datene dalla norma) sono soggetti agli adempimenti di pubblicità per tutta la parte di attività di pubblico interesse.
Successivamente, il D. Lgs. 33/2013, così come novellato dalla Legge 114/2014 (di conv. del D.L. 90/2014), ha esteso l'ambito di applicazione degli obblighi in materia di trasparenza individuati da detto decreto "limitatamente all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea, agli enti di diritto privato in controllo pubblico, ossia alle società e agli altri enti di diritto privato che esercitano funzioni amministrative, attività di produzione di beni e servizi a favore delle amministrazioni pubbliche o di gestione di servizi pubblici, sottoposti a controllo ai sensi dell'articolo 2359 del codice civile da parte di pubbliche amministrazioni".

IT City configurandosi quale ente di diritto privato in controllo pubblico, dovrà:

- collaborare con il Comune di Parma per assicurare la pubblicazione delle informazioni di cui ai commi 1 e 2 dell'art. 22 del D. Lgs. 33/2013;
- provvedere alla pubblicazione sul proprio sito istituzionale delle informazioni sugli incarichi di cui agli artt. 14 e 15 del D. Lgs. 33/2013;
- assicurare, per quanto compatibili alla propria struttura e attività, tutti gli adempimenti di trasparenza relativamente alle aree indicate nell'art. 1, comma 16, della Legge 190/2012, seguendo le prescrizioni del D. Lgs. 33/2013 (bilanci e conti consuntivi, costi unitari di realizzazione delle opere pubbliche e di produzione dei servizi erogati, informazioni relative ai procedimenti di autorizzazione o concessione, scelta del contraente per gli affidamenti, erogazioni di sovvenzioni, contributi, ecc., concorsi e prove selettive) in riferimento alla "attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea" (art. 11, comma 2, D.lgs. 33/2013).

4.3.2 *Compiti del Responsabile per la Trasparenza*

Il responsabile per la trasparenza, in conformità con quanto previsto dall'art. 43 del D. Lgs. 33/2013:

- provvede all'aggiornamento del programma triennale per l'attuazione effettiva degli obblighi di trasparenza, quale parte integrante del PTPC, all'interno del quale sono previste specifiche misure di monitoraggio sull'attuazione degli obblighi di trasparenza e ulteriori misure e iniziative di promozione della trasparenza;
- controlla e assicura la regolare attuazione dell'accesso civico.

4.3.3 *Responsabilità del Responsabile per la Trasparenza*

La responsabilità in caso di inadempimenti è disciplinata dagli artt. 46 e 47 del D. Lgs. 33/2013. In particolare nei casi di mancata o incompleta pubblicazione dei dati, l'inadempimento degli obblighi di pubblicazione o la mancata predisposizione del Programma triennale, costituisce elemento di valutazione della responsabilità dirigenziale. La responsabilità si esclude quando si dimostra che l'inadempimento è dipeso da causa non imputabile al responsabile.

4.4 Flussi informativi nei confronti degli Organismi di Controllo

Al fine di esercitare al meglio le proprie funzioni, gli Organismi di Controllo sono destinatari di qualsiasi informazione, documentazione, comunicazione che possa essere utile alla prevenzione dei reati. Si indicano di seguito alcune delle attività societarie del cui svolgimento i responsabili interni devono trasmettere informazioni e notizie:

- sostanziali cambiamenti dell'assetto operativo e di governance dell'azienda;
- attuazione del Modello e sanzioni interne irrogate in conseguenza della mancata osservanza dello stesso;
- operazioni finanziarie che assumano particolare rilievo per valore, modalità, rischiosità, atipicità;
- provvedimenti/sanzioni e richieste di informazioni provenienti da qualsiasi Autorità pubblica, relativi o attinenti ai reati contemplati dal D. Lgs. 231/2001 o dalla Legge 190/2012, o alle prescrizioni del D. Lgs. 33/2013;
- operazioni societarie straordinarie (fusioni, costituzione di nuove società ecc.) anche in ordine alle connesse adunanze dell'organo amministrativo;

Inoltre i responsabili interni devono tenere a disposizione degli Organismi di Controllo la documentazione inerente:

- avvenuta concessione di erogazioni pubbliche, rilascio di nuove licenze, di autorizzazioni o di altri rilevanti provvedimenti amministrativi;
- partecipazione a gare d'appalto ed aggiudicazione delle stesse e in genere instaurazione di rapporti contrattuali con la P.A.
- accertamenti fiscali del Ministero del Lavoro, degli Enti previdenziali e di ogni altra Autorità di Vigilanza.

4.5 Gestione delle segnalazioni verso gli Organismi di Controllo

Con la divulgazione del presente Modello in ambito aziendale è inoltre autorizzata la convergenza di qualsiasi segnalazione nei confronti degli Organismi di Controllo relativa alla temuta commissione di reati previsti dal Decreto 231/01 o dalla legge 190/2012 o a comportamenti non in linea con le regole di condotta stabilite nel Modello. Gli Organismi di Controllo, nel corso dell'attività di indagine, sono tenuti a garantire la dovuta riservatezza sull'origine delle informazioni ricevute, in modo da assicurare che i soggetti coinvolti non siano oggetto di ritorsioni, discriminazioni o penalizzazioni.
Tutte le segnalazioni devono essere conservate a cura degli Organismi di Controllo. La società, al fine di facilitare le segnalazioni, attiva opportuni canali di comunicazione dedicati (casella di posta elettronica):

- *Organismo di Vigilanza*: odv@itcity.it
- *Responsabile della Prevenzione della Corruzione*: anticorruzione@itcity.it
- *Responsabile della Trasparenza*: trasparenza@itcity.it

4.6 Flussi informativi dagli Organismi di controllo al top management

Gli organismi di controllo relazionano sulla loro attività periodicamente all'Amministratore Unico.
Le linee e la tempistica di reporting che sono obbligati a rispettare sono le seguenti:

- tutti gli Organismi di Controllo, su base continuativa direttamente all' Amministratore Unico per quel che riguarda particolari situazioni a rischio rilevate durante la propria attività di monitoraggio e che richiedono l'intervento della Società per l'adozione di eventuali azioni correttive/conoscitive da intraprendere;
- Gli Organismi di Controllo su base periodica (almeno annualmente con report scritto) all'Amministratore Unico in merito all'effettiva attuazione del Modello e del Piano Triennale di Prevenzione della Corruzione e della Trasparenza e in particolare:
    - rispetto delle prescrizioni previste, in relazione alle aree di rischio individuate;
    - eccezioni, notizie, informazioni e deviazioni dai comportamenti contenuti nel Codice Etico;
- tutti gli Organismi di Controllo, ad hoc, all'Amministratore Unico, in merito alla necessità di aggiornamento del Modello, del PTPCT e della mappatura delle aree a rischio in relazione a:
    - verificarsi di eventi organizzativi/operativi di rilievo;
    - cambiamenti nell'attività della Società;
    - cambiamenti nella organizzazione;
    - cambiamenti normativi;
    - altri eventi o circostanze tali da modificare sostanzialmente le aree a rischio cui è esposta la Società;
- tutti gli Organismi di Controllo, ad hoc, al Socio (al Responsabile della Prevenzione della Corruzione e/o al Responsabile Trasparenza), fatti sanzionabili ai sensi del D. Lgs. 231 o della legge 190/2012 commessi singolarmente dall' Amministratore Unico, o mancati o ritardati adempimenti previsti dal D. Lgs. 33/2013.

Gli Organismi di Controllo potranno essere invitati dall'Amministratore Unico in qualsiasi momento o potranno essi stessi presentare richiesta in tal senso, a riferire in merito al funzionamento del Modello o a situazioni specifiche rilevate nel corso della propria attività.

Qualora destinatario delle informazioni l'Amministratore Unico dovrà valutare quando sia appropriato informare il Socio (il Responsabile della Prevenzione della Corruzione e/o il Responsabile Trasparenza).

4.7 Il coordinamento con le direzioni aziendali

Tutte le direzioni e funzioni aziendali devono collaborare con gli Organismi di controllo, ed in particolare, devono rispondere tempestivamente alle richieste dallo stesso inoltrate, nonché mettere a disposizione tutta la documentazione ed ogni informazione necessaria allo svolgimento dell'attività di vigilanza.

4.8 Le risorse dell'Organismo di Vigilanza

L'Amministratore Unico assegna all'OdV le risorse umane e finanziarie ritenute opportune ai fini dello svolgimento dell'incarico assegnato.

L'OdV potrà disporre, per ogni esigenza necessaria al corretto svolgimento dei suoi compiti, del budget che l'Amministratore Unico provvede ad assegnargli con cadenza annuale, su proposta dell'OdV stesso.
Qualora se ne ravvisi l'opportunità, nel corso del proprio mandato, potrà chiedere all' Amministratore Unico, mediante comunicazione scritta motivata, l'assegnazione di ulteriori risorse umane e/o finanziarie.

Inoltre l'OdV potrà avvalersi, sotto la propria diretta sorveglianza e responsabilità, dell'ausilio di consulenti esterni, il cui compenso sarà corrisposto impiegando le risorse finanziarie assegnate all'OdV.

5. IL SISTEMA DISCIPLINARE

5.1 Sistema disciplinare

L'osservanza delle norme del Codice etico, delle misure contenute nel Modello di organizzazione e controllo previste dal D. Lgs. 231/01, delle prescrizioni previste, per la prevenzione della corruzione, dalla legge 190/2012 e delle prescrizioni previste dal D.Lgs. 33/2013 deve considerarsi parte essenziale delle obbligazioni contrattuali dei "Destinatari" di seguito definiti.
La violazione delle norme degli stessi lede il rapporto di fiducia instaurato con la Società e può portare ad azioni disciplinari, legali o penali; nei casi giudicati più gravi, la violazione può comportare la risoluzione del rapporto di lavoro, se posta in essere da un dipendente, ovvero l'interruzione del rapporto, se posta in essere da un soggetto terzo.
Per tale motivo è richiesto che ciascun Destinatario conosca le norme contenute nel Codice Etico e nel Modello (*Allegato 1 - Dichiarazione di responsabilità e di assenza di conflitti di interesse*), oltre alle norme di riferimento che regolano l'attività svolta nell'ambito della propria funzione.
Il presente sistema sanzionatorio, adottato anche ai sensi art. 6, comma secondo, lett. e) D. Lgs. 231/01 deve ritenersi complementare e non alternativo al sistema disciplinare stabilito dai C.C.N.L. vigenti ed applicabili alle diverse categorie di dipendenti in forza alla Società.
L'irrogazione di sanzioni disciplinari a fronte di violazioni del Modello 231 e del Codice Etico prescinde dall'eventuale instaurazione di un procedimento penale per la commissione di uno dei reati previsti dal Decreto.
Il sistema sanzionatorio e le sue applicazioni vengono costantemente monitorati dall'Organismo di Vigilanza.
Nessun procedimento disciplinare potrà essere archiviato, né alcuna sanzione disciplinare potrà essere irrogata, per violazione del Modello, senza preventiva informazione e parere dell'Organismo di Vigilanza.

5.2 Destinatari

5.2.1 Lavoratori subordinati

Il sistema sanzionatorio ha quali soggetti destinatari quelli legati alla società da un rapporto di subordinazione, tra i quali dirigenti, quadri, impiegati e operai.
In altri termini, il presente sistema sanzionatorio è inquadrato nel più ampio contesto del potere disciplinare del qua-le è titolare il datore di lavoro, ai sensi degli artt. 2106 c.c. e 7 della L. 300/70, sebbene il decreto stesso non contenga prescrizioni specifiche in merito alle sanzioni da adottare, limitandosi a prescrizioni di carattere generale.

5.2.2 Lavoratori parasubordinati

Il sistema sanzionatorio è destinato anche ai soggetti legati a Società IT.CITY da contratti di lavoro "parasubordinato", ossia dai contratti di lavoro previsti dal D. Lgs. 10.09.2003 n. 276, recante "Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui alla legge 14 febbraio 2003, n. 30", i quali non possono essere sottoposti al potere disciplinare della Società e alla conseguente irrogazione di sanzioni propriamente disciplinari.
La Società adotta con tali soggetti specifiche clausole contrattuali che impegnino gli stessi a non adottare atti e/o procedure che comportino violazioni del Codice Etico.
In tal modo, Società IT.CITY potrà sanzionare il mancato rispetto dei principi contenuti nel Codice Etico, nonché delle norme e degli standard generali di comportamento indicati nel Modello, ai sensi degli artt. 2222 ss. c.c.

5.2.3 Lavoratori autonomi - collaboratori e consulenti

Il sistema sanzionatorio deve altresì avere, quali soggetti destinatari, gli agenti di vendita, i collaboratori esterni, non-ché i soggetti esterni che a vario titolo, operano nell'interesse della Società.

5.2.4 Altri destinatari

Sono soggetti a sanzioni anche gli amministratori e tutti i partner che a vario titolo intrattengono rapporti con IT City.

5.3 Criteri di applicazione delle sanzioni

Il tipo e l'entità delle sanzioni specifiche saranno applicate nei singoli casi in base ai criteri generali di seguito indicati ed in proporzione alla gravità delle mancanze, fermo restando, in ogni caso, che il comportamento sarà considerato illecito disciplinare qualora sia effettivamente idoneo a produrre danni alla società.
I fattori rilevanti ai fini della irrogazione della sanzione sono:

- elemento soggettivo della condotta, a seconda del dolo o della colpa (negligenza, imprudenza, imperizia),
- rilevanza degli obblighi violati,
- entità del danno derivante alla Società o dall'eventuale applicazione delle sanzioni previste dal Decreto,
- livello di responsabilità gerarchica e/o tecnica,
- presenza di circostanze aggravanti o attenuanti con particolare riguardo alle precedenti prestazioni lavorative,
- eventuale condivisione di responsabilità con altri dipendenti che abbiano concorso nel determinare la mancanza,
- recidiva.

Nel caso in cui con un solo atto siano state commesse più infrazioni si applica la sanzione più grave.

5.4 Misure per i dipendenti

Le sanzioni previste di seguito si applicano nei confronti di quadri, impiegati ed operai, alle dipendenze della Società che pongano in essere illeciti disciplinari derivanti da:

- mancato rispetto delle misure previste dirette a garantire lo svolgimento dell'attività e/o a scoprire ed eliminare tempestivamente situazioni di rischio di reati, ex D. Lgs. 231/01 ed ex Legge 190/2012, nonché inosservanze di quanto previsto dal D. Lgs. 33/2013;
- mancata, incompleta o non veritiera rappresentazione dell'attività svolta relativamente alle modalità di documentazione, di conservazione e di controllo degli atti relativi alle procedure in modo da impedire la trasparenza e verificabilità delle stesse;
- violazione e/o elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di Vigilanza;
- inosservanza delle prescrizioni contenute nel Codice Etico;
- inosservanza delle disposizioni relative ai poteri di firma e del sistema delle deleghe, in relazione ai rischi connessi, con riguardo ad atti e documenti verso la Pubblica Amministrazione;
- inosservanza dell'obbligo di dichiarazioni periodiche (o falsità in dichiarazione) relative a: rispetto del Codice Etico e del Modello; assenza di conflitti di interessi, con riguardo a rapporti con la Pubblica Amministrazione;
- omessa vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità al fine di verificarne le azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato.

Il mancato rispetto delle misure e delle procedure indicate nel Modello, a seconda della gravità dell'infrazione, è sanzionato con i seguenti provvedimenti disciplinari:

a. richiamo verbale: verrà applicata la sanzione del richiamo verbale nei casi di violazione colposa dei principi del Codice Etico e/o di norme procedurali previste dal Modello o di errori procedurali, non aventi rilevanza esterna, dovuti a negligenza del lavoratore.
b. ammonizione scritta: verrà applicata nei casi di:
   - violazione colposa di norme procedurali previste dal Modello o di errori procedurali, aventi rilevanza esterna, dovuti a negligenza del lavoratore;
   - recidiva nelle violazioni di cui al punto a), per cui è prevista la sanzione del richiamo verbale.
c. multa per un importo fino a tre ore di retribuzione: oltre che nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione del rimprovero scritto, la multa potrà essere applicata nei casi in cui, per il livello di responsabilità gerarchico o tecnico, o in presenza di circostanze aggravanti, il comportamento colposo e/o negligente possa minare, sia pure a livello potenziale, l'efficacia del Modello; quali a titolo esemplificativo ma non esaustivo:
   - l'inosservanza delle procedure previste dal Modello riguardanti un procedimento in cui una delle parti necessarie è la Pubblica Amministrazione;
   - reiterate violazioni di cui al precedente punto b), per cui è prevista la sanzione dell'ammonizione scritta;

d. sospensione dal lavoro e dalla retribuzione fino a 3 giorni: verrà applicata, oltre che nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione della multa, nei casi di gravi violazioni procedurali tali da esporre la Società a responsabilità nei confronti dei terzi. A titolo esemplificativo ma non esaustivo si applica in caso di:
   - inosservanza dell'obbligo delle dichiarazioni periodiche (o falsità in dichiarazione) relative al rispetto del Codice Etico e del Modello; delle dichiarazioni relative all'assenza di conflitti di interessi, con riguardo a rapporti con la Pubblica Amministrazione e delle attestazioni scritte richieste dalla procedura relativa al processo di bilancio;
   - inosservanza delle disposizioni relative ai poteri di firma e del sistema delle deleghe, in relazione ai rischi connessi, con riguardo ad atti e documenti verso la P.A.;
   - omessa vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità al fine di verificare le loro azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato;
   - reiterate violazioni di cui al precedente punto c).

   Ove i dipendenti sopra indicati siano muniti di procura con potere di rappresentare all'esterno la Società, l'applicazione della sanzione descritta comporterà anche la revoca automatica della procura stessa.
e. licenziamento con preavviso: verrà applicata nei casi di reiterata grave violazione delle procedure aventi rilevanza esterna nello svolgimento di attività che implicano rapporti giudiziali, negoziali ed amministrativi con la P.A., nonché di reiterata inosservanza delle prescrizioni contenute nel Codice Etico e del Modello 231, di cui al precedente punto d).
f. licenziamento senza preavviso : Verrà applicata per mancanze commesse dolosamente e così gravi da non consentire la prosecuzione anche provvisoria del rapporto di lavoro, quali a titolo esemplificativo, ma non esaustivo:
   - violazione dolosa di procedure aventi rilevanza esterna e/o elusione fraudolenta realizzata attraverso un comportamento inequivocabilmente diretto alla commissione di un reato ricompreso fra quelli previsti dal Decreto tale da far venir meno il rapporto fiduciario con il datore di lavoro;
   - violazione e/o elusione del sistema di controllo, poste in essere con dolo mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di Vigilanza;
   - mancata, incompleta o non veritiera documentazione dell'attività svolta relativamente alle modalità di documentazione e di conservazione degli atti delle procedure, dolosamente diretta ad impedire la trasparenza e verificabilità delle stesse
   - mancata segnalazione dello stato di contenzioso con la Pubblica Amministrazione.

In ogni caso, qualora il lavoratore sia incorso in una delle mancanze di cui al presente punto f) la Società potrà disporre, in attesa del completo accertamento delle violazioni, la sospensione cautelare non disciplinare del medesimo con effetto immediato per un periodo non superiore a 6 giorni.
Nel caso in cui la Società decida di procedere al licenziamento, lo stesso avrà effetto dal giorno in cui ha avuto inizio la sospensione cautelare.

Il datore di lavoro non potrà comminare alcuna sanzione al lavoratore senza avergli preventivamente contestato l'addebito e senza aver sentito la sua difesa.

La contestazione del datore di lavoro, salvo che per il richiamo verbale, dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno essere comminati prima che siano trascorsi 5 giorni, nel corso dei quali il lavoratore potrà presentare la sua difesa. Se entro ulteriori 5 giorni non viene adottato alcun provvedimento, si riterranno accolte le giustificazioni del lavoratore.

La difesa del lavoratore può essere effettuata anche verbalmente, anche con l'assistenza di un rappresentante dell'associazione sindacale cui aderisce.

La comminazione del provvedimento dovrà essere motivata e comunicata per iscritto.
I provvedimenti, fatta eccezione del richiamo verbale, possono essere impugnati dal lavoratore, in sede sindacale, secondo le norme contrattuali relative alle vertenze.

5.5 Misure per i dirigenti

Anche nei confronti dei dirigenti che attuino comportamenti in violazione delle prescrizioni del presente Modello, verranno adottate le misure più idonee in conformità a quanto previsto dal regolamento di disciplina dello Statuto dei Lavoratori.
I provvedimenti disciplinari applicabili ai dirigenti sono quelli previsti dalle norme contrattuali collettive dei CCNL e dalle norme legislative in vigore per gli impiegati di massima categoria dipendenti dell'azienda cui il dirigente appartiene, che rimandano per lo più al Codice Civile, anche in relazione a quanto previsto per la risoluzione del contratto (art. 2119).
Tenuto conto della natura fiduciaria del rapporto di lavoro, il mancato rispetto delle disposizioni previste dal Modello e dal Codice Etico, è sanzionato considerando in sede applicativa il principio di proporzionalità previsto dall'art. 2106 del Codice Civile e valutando, per ciascuna fattispecie, la gravità oggettiva del fatto costituente infrazione disciplinare, il grado di colpa, l'eventuale reiterazione di un medesimo comportamento, nonché l'intenzionalità del comportamento stesso.

5.6 Misure nei confronti di lavoratori autonomi

L'inosservanza delle prescrizioni contenute nel Modello e nel Codice Etico da parte di ciascun lavoratore autonomo può determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, fermo restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal Decreto.
In particolare, si rende necessaria l'utilizzazione di un'apposita clausola contrattuale, che formerà oggetto di espressa accettazione da parte del terzo contraente e, quindi, parte integrante degli accordi contrattuali.
Con questa clausola, tali collaboratori dichiareranno di essere a conoscenza, di accettare e di impegnarsi a rispettare il Codice Etico ed il Modello adottati dalla Società, di aver eventualmente adottato anch'essi un analogo Codice Etico e Modello e di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Modello di cui al D. Lgs. 231/2001 e alla Legge 190/2012.
Nel caso in cui tali soggetti siano stati implicati nei procedimenti di cui sopra, dovranno dichiararlo ai fini di una maggiore attenzione da parte della società, qualora si addivenga all'instaurazione del rapporto.
Nel rispetto della correttezza e buona fede nell'esecuzione del contratto, fatta salva la disciplina di legge, la Società, in caso di violazione di una raccomandazione da parte di un collaboratore o consulente, può:

- contestare l'inadempimento al destinatario con la contestuale richiesta di adempimento degli obblighi contrattualmente assunti e previsti dal presente Codice di Comportamento, se del caso, concedendo un termine ovvero immediatamente, nonché
- richiedere un risarcimento del danno pari al corrispettivo percepito per l'attività svolta nel periodo decorrente dalla data dell'accertamento della violazione della raccomandazione all'effettivo adempimento.

Fatta salva la disciplina di legge, in caso di violazione di n° 3 (tre) divieti contenuti nel Codice Etico o nel Modello, la Società può:

- risolvere automaticamente il contratto in essere per grave inadempimento, ex art. 1453 c.c. nonché
- richiedere un risarcimento del danno pari al corrispettivo percepito per l'attività svolta nel periodo decorrente dalla data dell'accertamento della terza violazione di raccomandazione o della violazione del divieto alla data di comunicazione della risoluzione.

5.7 Misure nei confronti degli amministratori

La disciplina sanzionatoria per gli Amministratori considera come applicabile quanto previsto dal codice civile; a norma dell'art. 2392 c.c. gli Amministratori sono responsabili verso la società se non adempiono ai doveri imposti dalla legge con la dovuta diligenza; essi sono solidalmente responsabili verso la società dei danni derivanti dall'inosservanza di tali doveri. Nel caso di violazioni delle disposizioni contenute nel Modello, da parte di un Amministratore, l'Organismo di Vigilanza darà informazione all'Assemblea dei Soci ed al Collegio Sindacale, affinché siano presi gli opportuni provvedimenti, in conformità alla normativa, ovvero alle prescrizioni adottate da IT City, nel codice sanzionatorio. Pertanto, in relazione al danno cagionato da specifici eventi pregiudizievoli, strettamente riconducibili al mancato esercizio della dovuta diligenza, potrà correlarsi l'esercizio di un'azione di responsabilità sociale ex art. 2393 c.c. e seguenti a giudizio dell'Assemblea.

6. Comunicazione e Formazione

In relazione alle previsioni normative e conformemente alla giurisprudenza di merito, perché il Modello abbia efficacia come strumento di prevenzione e controllo, è necessario che siano svolti un piano di comunicazione informativa e un piano di formazione interno indirizzati al personale ed ai consulenti esterni e a quanti, sulla base dei rapporti intrattenuti con la Società, possano mettere in atto comportamenti a rischio di commissione di reati ex D. Lgs. 231/01, Legge 190/2012 e D. Lgs.33/2013.

6.1 Piano di comunicazione interna

Il Modello è comunicato a cura dell'Amministratore Unico attraverso i mezzi ritenuti più opportuni (es. bacheca aziendale, invio per posta elettronica, etc.), ivi compreso il sistema intranet aziendale, a tutti i soggetti che ne sono destinatari. Agli apicali in generale, ai dipendenti, alle risorse in outsourcing, ai collaboratori esterni verrà inviata una comunicazione con la quale:

- si informa dell'avvenuta approvazione del Modello di organizzazione e controllo ai sensi del D.Lgs. 231/01 da parte dell'Amministratore Unico, o del suo aggiornamento;
- si comunica la nomina dell'OdV, o sua modifica;
- si comunica la nomina del RPC, o sua modifica;
- si comunica la nomina del RT, o sua modifica;
- si invita a consultare copia del Modello 231 inviato in formato elettronico o copia cartacea conservata presso la sede della società;
- si richiede la conoscenza della norma nei suoi contenuti essenziali e dei reati richiamati dalla stessa.

6.2 Piano di comunicazione esterna

La Società IT.CITY si impegna a comunicare l'avvenuta adozione del Modello ai principali fornitori, consulenti esterni e terzi in generale con i quali collabora abitualmente, e prevedere l'inserimento della clausola 231 all'interno del contratti.

6.3 Piano di formazione

Tutti i soggetti interni destinatari del Modello dovranno essere istruiti in merito ai comportamenti da tenere al fine di prevenire situazioni a rischio di reato ex D. Lgs. 231/2001, Legge 190/2012 e D. Lgs. 33/2013.
Il piano di formazione è predisposto dall'Organismo di Vigilanza, di concerto con il Responsabile della Prevenzione della Corruzione e con il Responsabile della Trasparenza.
Il piano di formazione pluriennale contemplerà i seguenti argomenti:

- Reati previsti dal D. Lgs. 231/2001, aree a rischio, obiettivi e contenuti del Modello;
- Legge 190/2012 e prevenzione della corruzione;
- D. Lgs. 33/2913 e obblighi di trasparenza;
- Aggiornamenti a cadenza periodica, in relazione ad integrazioni normative, modifiche organizzative e/o procedurali;
- Informativa nella lettera di assunzione ed un seminario per i neoassunti.

La partecipazione ai suddetti programmi di formazione è tracciata e obbligatoria.
L'Organismo di Vigilanza cura, d'intesa con l'Organo Amministrativo, che il programma di formazione sia adeguato ed efficacemente attuato. Le iniziative di formazione possono svolgersi anche a distanza o mediante l'utilizzo di sistemi informatici.
La Società IT.CITY provvederà a rendere noto, nel corso di tali attività formative, che i destinatari della formazione sono tenuti a conoscere i contenuti del Modello, a contribuire, in relazione al ruolo ed alle responsabilità rivestite, alla loro corretta attuazione ed a segnalare eventuali carenze agli Organismi di Controllo, attraverso indirizzo e-mail:

- odv@itcity.it
- anticorruzione@itcity.it
- trasparenza@itcity.it

I soggetti destinatari dei corsi di formazione sono tenuti a parteciparvi e la mancata partecipazione, senza una giusta motivazione, è considerata comportamento sanzionabile.

PARTE SPECIALE

1. Introduzione

Ai sensi di quanto disposto dal Decreto, la Società, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. *control and risk self assessment*), ha identificato le attività sensibili (suddivise per tipologia di reato ed elencate nei paragrafi successivi), nell'ambito delle quali possano essere potenzialmente commessi reati tra quelli previsti dal Decreto.

Al fine di prevenire o di mitigare il rischio di commissione di tali reati, la Società ha dunque formulato dei principi generali di comportamento e dei protocolli generali di prevenzione applicabili a tutte le attività sensibili e dei protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate.

2. Principi generali di comportamento

Tutti i destinatari del Modello, così come individuati nel paragrafo 3.6 della Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento, nel Codice Etico e nel PTPCT, al fine di prevenire il verificarsi di reati previsti dal Decreto.

Ai fini dell'adozione e dell'attuazione del Modello di organizzazione, gestione e controllo, la Società attua inoltre i protocolli di seguito indicati.

3. Protocolli generali di prevenzione

Nell'ambito di tutte le operazioni che concernono le attività sensibili, di cui ai successivi paragrafi, si attuano i seguenti protocolli generali di prevenzione:

- sono legittimati a svolgere le attività sensibili solo i soggetti che siano stati preventivamente identificati mediante deleghe, procure, organigrammi, job description, procedure o eventuali disposizioni organizzative;
- sono legittimati a trattare con la Pubblica Amministrazione soggetti che siano stati previamente identificati a tale scopo;
- la formazione e l'attuazione delle decisioni della Società rispondono ai principi e alle prescrizioni contenute nelle disposizioni di legge, nell'atto costitutivo e nel Codice Etico della Società;
- sono formalizzate le responsabilità di gestione, coordinamento e controllo all'interno della Società;
- sono formalizzati i livelli di dipendenza gerarchica e sono descritte le diverse mansioni presenti all'interno della Società;
- le fasi di formazione e i livelli autorizzativi degli atti della Società sono sempre documentati e ricostruibili;
- il sistema di deleghe e poteri di firma verso l'esterno è coerente con le responsabilità assegnate e la conoscenza di tali poteri da parte dei soggetti esterni è garantita da strumenti di comunicazione e di pubblicità adeguati;
- 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 operazioni economiche;
- non vi è identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono darne evidenza contabile e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- per tutte le operazioni a rischio che concernono le attività sensibili sono implementate ed attuate procedure e linee guida ed è individuato un Responsabile interno per l'attuazione dell'operazione, che corrisponde,

salvo diversa indicazione, al Responsabile della Funzione competente per la gestione dell'operazione a rischio considerata. Il Responsabile interno:

- può chiedere informazioni e chiarimenti a tutte le funzioni aziendali, alle unità operative o ai singoli soggetti che si occupano o si sono occupati dell'operazione a rischio;
- informa tempestivamente l'Organismo di Vigilanza di qualunque criticità o conflitto di interessi;
- può interpellare l'Organismo di Vigilanza in tutti i casi di inefficacia, inadeguatezza o difficoltà di attuazione dei protocolli di prevenzione o delle procedure operative di attuazione degli stessi o al fine di ottenere chiarimenti in merito agli obiettivi e alle modalità di prevenzione previste dal Modello;

- l'accesso ai dati della Società è conforme al Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni o integrazioni, anche regolamentari;
- i documenti riguardanti la formazione delle decisioni e l'attuazione delle stesse sono archiviati e conservati a cura della funzione competente. L'accesso ai documenti già archiviati è consentito solo alle persone autorizzate in base alle procedure operative aziendali, nonché al collegio sindacale, alla società di revisione e all'Organismo di Vigilanza;
- la scelta di eventuali consulenti esterni è motivata e avviene sulla base di requisiti di professionalità, indipendenza e competenza;
- i sistemi di remunerazione premianti per Dipendenti e collaboratori rispondono ad obiettivi realistici e coerenti con le mansioni, con le attività svolte e con le responsabilità affidate;
- i flussi finanziari della Società, sia in entrata sia in uscita, sono costantemente monitorati e sempre tracciabili;
- tutte le forme di liberalità finalizzate a promuovere l'immagine e l'attività della Società devono essere autorizzate, giustificate e documentate;
- l'Organismo di Vigilanza verifica che le procedure operative aziendali che disciplinano le attività a rischio, che costituiscono parte integrante del Modello organizzativo aziendale, diano piena attuazione ai principi e alle prescrizioni contenuti nella presente Parte Speciale, e che le stesse siano costantemente aggiornate, anche su proposta dell'Organismo, al fine di garantire il raggiungimento delle finalità del presente documento.

4. Attività strumentali alla commissione di reati e protocolli specifici di prevenzione

La Società, inoltre, ha individuato le attività strumentali alla commissione dei reati, cioè le attività nelle quali sussiste non – o non solo – la possibilità di commissione di alcuni dei reati previsti dal Decreto, ma tramite le quali possono essere create provviste di denaro (o di altre utilità) finalizzate alla commissione dei reati di corruzione, verso pubblici ufficiali, incaricati di un pubblico servizio o privati.

Tali attività sono le seguenti:

- ✓ Gestione delle risorse finanziarie (tramite Home banking);
- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Conferimento e gestione delle consulenze;
- ✓ Gestione del processo di assunzione e gestione del personale (tramite selezione pubblica);
- ✓ Gestione delle note spese;
- ✓ Gestione dei beni strumentali (es. PC, schede SIM).

A tali attività, oltre ai principi generali di comportamento e ai protocolli generali di prevenzione di cui ai paragrafi precedenti, si applicano i protocolli specifici di prevenzione che seguono.

Per le operazioni riguardanti la **gestione delle risorse finanziarie (tramite Home banking)**, i protocolli prevedono che:

- siano stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative;
- delle modifiche ai limiti stabiliti dall'autonomo impiego sia data informazione al Collegio Sindacale;
- le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie abbiano una causale espressa, siano motivate, documentate e registrate in conformità ai principi di correttezza professionale e contabile;
- siano vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minime di spesa (piccola cassa) espressamente autorizzate dai Responsabili delle Funzioni competenti come previsto nella procedura aziendale applicabile;
- con riferimento alle operazioni bancarie e finanziarie, la Società si avvalga solo di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;
- i pagamenti a terzi siano effettuati mediante circuiti bancari con mezzi che garantiscano evidenza che il beneficiario del pagamento sia effettivamente il soggetto terzo contraente con la Società;
- il rimborso delle spese sostenute dai collaboratori sia richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute, nel rispetto della procedura aziendale applicabile;
- gli incassi e i pagamenti della Società nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente.

Per le operazioni riguardanti la **gestione degli approvvigionamenti (beni, servizi, appalti, software)**, si rimanda al "Regolamento per la disciplina di lavori, forniture, servizi e spese in economia e dei relativi contratti" adottato dalla Società.

Inoltre, i protocolli prevedono che:

- siano individuati degli indicatori di anomalia che consentano di rilevare eventuali transazioni "a rischio" o "sospette" con fornitori sulla base del:
  - profilo soggettivo della controparte (ad es. esistenza di precedenti ex D.Lgs 231/01; reputazione opinabile; ammissioni o dichiarazioni da parte della controparte in ordine al proprio coinvolgimento in attività criminose);
  - comportamento della controparte (ad es. comportamenti ambigui, mancanza di dati occorrenti per la realizzazione delle transazioni o reticenza a fornirli);
  - dislocazione territoriale della controparte (ad es. transazioni effettuate in paesi off-shore);
  - profilo economico-patrimoniale dell'operazione (ad es. operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica);
  - caratteristiche e finalità dell'operazione (ad es. uso di prestanomi, modifiche delle condizioni contrattuali standard, finalità dell'operazione).
- la scelta e la valutazione della controparte avvenga nel rispetto della normativa applicabile in tema di gestione degli appalti (Codice Appalti vigente) e delle normative in materia di trasparenza e anticorruzione;
- vi sia il coinvolgimento di una pluralità di soggetti nella fase di negoziazione dell'accordo e di assegnazione dell'incarico di fornitura, nel rispetto delle procedure e delle normative vigenti;
- il Responsabile della Funzione coinvolta che approva l'accordo:

- conservi la documentazione relativa all'operazione in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- informi l'OdV di qualsiasi criticità possa riscontrarsi (ai sensi del D.Lgs 231/01);

- i contratti di approvvigionamento siano sempre preventivamente valutati e autorizzati dai soggetti dotati di idonei poteri;
- il Responsabile della funzione interessata dall'appalto segnali immediatamente all'Organismo di Vigilanza eventuali anomalie nelle prestazioni rese dall'appaltatore o dal fornitore o particolari richieste avanzate alla Società da questi soggetti, connessi e potenziali rischi ex. D.Lgs 231/01;
- le fatture ricevute dalla Società relative all'acquisto di beni o di servizi siano registrate esclusivamente a fronte di idonea evidenza della stipula del contratto o della effettiva ricezione della merce o del servizio.

Per le operazioni riguardanti il **conferimento e gestione delle consulenze**, si rimanda al "Regolamento per la disciplina di lavori, forniture, servizi e spese in economia e dei relativi contratti" adottato dalla Società.

Inoltre, i protocolli prevedono che:

- i soggetti cui conferire incarichi di consulenza siano scelti in base ai requisiti di professionalità, indipendenza e competenza, nel rispetto delle normative applicabili;
- l'affidamento degli incarichi avvenga nel rispetto delle procedure, delle autorizzazioni e dei controlli interni adottati dalla Società e delle normative applicabili;
- non vi sia identità soggettiva tra chi richiede l'affidamento degli incarichi e chi l'autorizza;
- l'incarico sia conferito per iscritto con indicazione del compenso pattuito e del contenuto della prestazione;
- al termine dell'incarico sia richiesto al consulente / professionista di dettagliare per iscritto le prestazioni effettuate;
- al fine di autorizzare il pagamento della prestazione, la Funzione richiedente certifichi l'avvenuta prestazione prima del pagamento stesso, nel rispetto delle normative applicabili;
- non siano corrisposti compensi in misura non congrua rispetto alle prestazioni rese alla Società o non conformi all'incarico conferito, alle condizioni o prassi esistenti sul mercato o alle tariffe professionali vigenti per la categoria interessata.

Per le operazioni riguardanti la **gestione del processo di assunzione e gestione del personale (tramite selezione pubblica)**, i protocolli prevedono che:

- la selezione e assunzione del personale sia svolta nel rispetto della normativa applicabile vigente;
- la richiesta sia autorizzata dal Responsabile competente secondo le procedure interne e nel rispetto della normativa applicabile vigente.

Per le operazioni riguardanti la **gestione delle note spese**, i protocolli prevedono che:

- il rimborso delle spese sostenute, che includono anche le spese di rappresentanza, debba essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione, giustificativa delle spese sostenute;
- sia individuato, secondo i livelli gerarchici presenti in azienda, il responsabile che autorizza ex ante o ex post le note spese ai soggetti richiedenti;
- le note spese siano gestite nel rispetto delle procedure applicabili.

Per le operazioni riguardanti la **gestione dei beni strumentali (es. PC, schede SIM)**, i protocolli prevedono che:

- l'assegnazione del bene strumentale sia motivata, in ragione del ruolo e della mansione del personale beneficiario e sia autorizzata dalla funzione competente;
- siano identificati i beni strumentali e le utilità aziendali concessi (ad es. personal computer, schede SIM, ecc.);
- venga mantenuto un inventario aggiornato dei beni attribuiti agli assegnatari;
- siano previsti casi di revoca del bene assegnato in caso di violazione delle procedure o regolamenti aziendali durante il loro utilizzo;
- siano stabilite le modalità di restituzione dei beni in caso di dimissioni/licenziamento.

SEZIONE A

REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E REATI DI CORRUZIONE

(artt. 24 e 25 del Decreto e Legge 190/2012)

A.1 Premessa

Il concetto di Pubblica Amministrazione in diritto penale viene inteso in senso ampio, comprendendo l'intera attività dello Stato e degli altri enti pubblici; pertanto, i reati contro la Pubblica Amministrazione perseguono fatti che impediscono o turbano il regolare svolgimento non solo dell'attività – in senso tecnico – amministrativa, ma anche di quella legislativa e giudiziaria. Viene quindi tutelata la Pubblica Amministrazione intesa come l'insieme di tutte le funzioni pubbliche dello Stato o degli altri enti pubblici.

I soggetti che rappresentano la Pubblica Amministrazione ai fini del diritto penale sono coloro che svolgono una funzione pubblica o un pubblico servizio.

Per funzione pubblica si intendono le attività disciplinate da norme di diritto pubblico che attengono alle funzioni legislativa (Stato, Regioni, Province a statuto speciale, Comuni, ecc.), amministrativa (membri delle amministrazioni statali e territoriali, Forze dell'Ordine, membri delle amministrazioni sovranazionali, membri delle Authority, delle Camere di Commercio, membri di Commissioni Edilizie, collaudatori di opere pubbliche, periti del Registro Navale Italiano, ecc.), giudiziaria (giudici, ufficiali giudiziari, organi ausiliari dell'Amministrazione della Giustizia quali curatori o liquidatori fallimentari, ecc.).

La funzione pubblica è caratterizzata dall'esercizio di:

- **potere autoritativo**, cioè di quel potere che permette alla Pubblica Amministrazione di realizzare i propri fini mediante veri e propri comandi, rispetto ai quali il privato si trova in una posizione di soggezione. Si tratta dell'attività in cui si esprime il c.d. potere d'imperio, che comprende sia il potere di coercizione (arresto, perquisizione, ecc.) e di contestazione di violazioni di legge (accertamento di contravvenzioni, ecc.), sia i poteri di supremazia gerarchica all'interno di pubblici uffici;
- **potere certificativo**, cioè il potere del certificatore di attestare un fatto con efficacia probatoria.

Per pubblico servizio si intendono attività disciplinate da norme di diritto pubblico, caratterizzate dalla mancanza dei poteri autoritativi o certificativi tipici della funzione pubblica, con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

I soggetti che svolgono una funzione pubblica o un pubblico servizio sono denominati pubblici ufficiali o incaricati di pubblico servizio.

Il pubblico ufficiale è colui che può formare o manifestare la volontà della Pubblica Amministrazione ovvero esercitare poteri autoritativi o certificativi.

A titolo esemplificativo e non esaustivo si considerano pubblici ufficiali i membri delle amministrazioni statali e territoriali, i membri delle amministrazioni sovranazionali (ad esempio dell'Unione Europea), i NAS, i membri delle Autorità di Vigilanza, il personale di vigilanza della Asl, i membri delle Forze dell'Ordine e della Guardia di Finanza, i membri delle Camere di Commercio, gli amministratori di enti pubblici economici, i membri delle Commissioni Edilizie, i giudici, gli ufficiali giudiziari, gli organi ausiliari dell'Amministrazione della Giustizia (ad esempio, i curatori fallimentari).

L'incaricato di pubblico servizio svolge invece le attività attinenti la cura di interessi pubblici o il soddisfacimento di bisogni di interesse generale assoggettate alla vigilanza di un'autorità pubblica. La giurisprudenza penalistica ha chiarito che l'inquadramento burocratico del soggetto nella struttura di un ente pubblico non costituisce criterio per riconoscere la qualifica di incaricato di pubblico servizio, poiché ciò che rileva è l'attività in concreto svolta dal soggetto. Pertanto, anche un privato o il dipendente di una società privata può essere qualificato quale incaricato di pubblico servizio quando svolge attività finalizzate al perseguimento di uno scopo pubblico e alla tutela di un interesse pubblico.

A titolo esemplificativo e non esaustivo possono essere considerati incaricati di pubblico servizio i Dipendenti del SSN, gli addetti all'ufficio cassa di un ente pubblico, i Dipendenti di enti ospedalieri, dell'ASL, dell'INAIL,

dell'INPS, i Dipendenti di aziende energetiche municipali, banche, uffici postali, uffici doganali, i membri dei consigli comunali, i Dipendenti delle Ferrovie dello Stato, dell'ENI e di concessionari autostradali.

A.2 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerate applicabili alla Società le disposizioni concernenti i seguenti reati contro la Pubblica Amministrazione (art. 24 e 25 del Decreto) e reati di corruzione ex Legge 190/2012:

a) **Peculato (con esclusione dell'ipotesi dell'uso momentaneo del bene)**, di cui all'art. 314 comma 1 c.p. e costituito dalla condotta del pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria, purché il fatto offenda gli interessi finanziari dell'Unione europea;

b) **peculato mediante profitto dell'errore altrui**, di cui all'art. 316 c.p. e costituito dalla condotta del pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, purché il fatto offenda gli interessi finanziari dell'Unione europea;

c) **malversazione a danno dello Stato**, di cui all'art. 316-*bis* c.p. e costituito dalla condotta di chi, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità;

d) **indebita percezione di erogazioni a danno dello Stato**, di cui all'art. 316-*ter* c.p. e costituito dalla condotta di chi, salvo che il fatto costituisca il reato previsto dall'articolo 640-*bis* c.p., mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea;

e) **frode nelle pubbliche forniture**, di cui all'art. 356 c.p. e costituito dalla condotta di chi commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo 355 c.p. (ossia gli obblighi che derivano da un contratto di fornitura concluso con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità);

f) **truffa a danno dello Stato o di un altro ente pubblico**, di cui all'art. 640 c.p., comma 2, n. 1 c.p. e costituito dalla condotta di chi, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;

g) **truffa aggravata per il conseguimento di erogazioni pubbliche**, di cui all'art. 640-*bis* c.p. e costituito dalla stessa condotta di cui al punto precedente, se posta in essere per ottenere contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee;

h) **frode informatica in danno dello Stato o di altro ente pubblico**, di cui all'art. 640-*ter* c.p. e costituito dalla condotta di chi, alterando in qualsiasi modo il funzionamento di un sistema informatico, o telematico, o intervenendo senza diritto con qualsiasi modalità su dati, informazioni, o programmi contenuti in un sistema informatico, o telematico, o ad esso pertinenti, procura a sé, o ad altri, un ingiusto profitto, con danno dello Stato o di altro ente pubblico;

i) **concussione**, di cui all'art. 317 c.p. e costituito dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità;

j) **corruzione per l'esercizio della funzione**, di cui all'art. 318 c.p. e costituito dalla condotta del pubblico ufficiale il quale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa;

k) **corruzione per un atto contrario ai doveri d'ufficio**, di cui all'art. 319 c.p. e costituito dalla condotta del pubblico ufficiale il quale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa;

l) **corruzione in atti giudiziari**, di cui all'art. 319-*ter* c.p. e costituito dai fatti di corruzione, qualora commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo;

m) **induzione indebita a dare o promettere utilità**, di cui all'art. 319-*quater* c.p. e costituito dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, salvo che il fatto costituisca più grave reato, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, nonché dalla condotta di colui che dà o promette il denaro o altra utilità;

n) **corruzione di persona incaricata di un pubblico servizio**, di cui all'art. 320 c.p., e costituito dalle condotte di cui agli artt. 318 e 319 c.p. qualora commesse dall'incaricato di un pubblico servizio;

ai sensi dell'art. 321 c.p. (**pene per il corruttore**), le pene stabilite agli artt. 318, comma 1, 319, 319-*bis*, 319-*ter* e 320 c.p. in relazione alle ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità;

o) **istigazione alla corruzione**, promette denaro o altra utilità non dovuti a un pubblico ufficiale o a un incaricato di un pubblico servizio per l'esercizio delle sue funzioni o dei suoi poteri, o per indurre lo stesso a omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata, nonché dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri o che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'art. 319 c.p.;

p) **corruzione, induzione indebita a dare o promettere utilità e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri**, di cui all'art. 322-*bis* c.p., in base al quale le disposizioni di cui agli artt. da 317 a 320 e 322, commi 3 e 4, c.p. si applicano anche:

- ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

Le disposizioni di cui agli artt. 319-*quater*, comma 2, 321 e 322, commi 1 e 2 c.p., si applicano anche se il denaro o altra utilità sono dati, offerti o promessi:

- alle persone indicate nel primo comma dell'art. 322-*bis*;
- a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria.

Le persone indicate nel primo comma dell'art. 322-*bis* sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

q) **abuso d'ufficio**, di cui all'art. 323 c.p. e costituito dalla condotta, salvo che il fatto non costituisca un più grave reato, del pubblico ufficiale o dell'incaricato di pubblico servizio che, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti , intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto, purché il fatto offenda gli interessi finanziari dell'Unione europea;

r) **utilizzazione d'invenzioni o scoperte conosciute per ragioni di ufficio**, di cui all'art 325 c.p. e costituito dalla conditta del pubblico ufficiale, o dell'incaricato di un pubblico servizio che impiega, a proprio o altrui profitto, invenzioni o scoperte scientifiche, o nuove applicazioni industriali, che egli conosca per ragione dell'ufficio o servizio, e che debbano rimanere segrete;

s) **rivelazione ed utilizzazione di segreti di ufficio**, di cui all'art 326 c.p. e costituito dalla condotta del pubblico ufficiale o della persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza;

t) **corruzione tra privati,** di cui all'art. 25 ter del D. Lgs. 231/01, si rimanda alla Sezione E della Parte Speciale del Modello.

A.3 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati reati nei rapporti con la Pubblica Amministrazione previsti dagli artt. 24 e 25 del Decreto:

- ✓ Gestione dei rapporti con i rappresentanti della PA in occasione di accertamenti, ispezioni e verifiche (es. Agenzia delle Entrate; Guardia di Finanza), anche tramite consulenti esterni;
- ✓ Gestione dei rapporti con l'Autorità Giudiziaria, anche tramite consulenti esterni;
- ✓ Gestione del contratto di servizio per la gestione del Sistema Informativo con il Comune di Parma;
- ✓ Richiesta di autorizzazioni, di concessioni e di certificazioni;
- ✓ Richiesta, gestione, monitoraggio di contributi, esenzioni e agevolazioni fiscali, ecc., anche tramite consulenti esterni;
- ✓ Pubbliche relazioni che comportano rapporti con la PA (es. partecipazioni a convegni, meeting con enti pubblici);
- ✓ Gestione delle risorse finanziarie (tramite Home banking);
- ✓ Gestione del credito e del contenzioso contrattuale, anche tramite consulenti esterni;
- ✓ Gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer;
- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Conferimento e gestione delle consulenze;
- ✓ Gestione del processo di assunzione e gestione del personale (tramite selezione pubblica);
- ✓ Gestione delle note spese;
- ✓ Gestione dei beni strumentali (es. PC, schede SIM);
- ✓ Gestione del processo di creazione, trattamento e archiviazione di documenti elettronici con valore probatorio.

A.4 Principi generali di comportamento

Nello svolgimento delle attività sensibili, tutti i Destinatari del Modello sono tenuti ad osservare i principi generali di comportamento che la Società ha individuato in conformità anche a quanto previsto dal Codice Etico.

Questi principi sono qui di seguito indicati:

- è vietato tenere rapporti con la Pubblica Amministrazione, se non da parte dei soggetti a ciò deputati secondo l'organigramma della Società (che indica anche le funzioni svolte), ordini di servizio o eventuali deleghe e procure;
- è fatto divieto di offrire/ricevere o effettuare, direttamente o indirettamente, pagamenti indebiti e promesse di vantaggi personali, di qualsiasi natura, ai rappresentanti della Pubblica Amministrazione italiana

e straniera. Tale divieto include l'offerta, diretta o indiretta, di gratuita disponibilità di servizi, finalizzata a influenzare decisioni o transazioni;

- è vietato distribuire ai rappresentanti della Pubblica Amministrazione italiana e straniera omaggi o regali, salvo che si tratti piccoli omaggi di modico o di simbolico valore, e tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere considerati finalizzati all'acquisizione impropria di benefici;
- è vietato presentare ad organismi pubblici nazionali e stranieri dichiarazioni non veritiere o prive delle informazioni dovute nell'ottenimento di finanziamenti pubblici, ed in ogni caso compiere qualsivoglia atto che possa trarre in inganno l'ente pubblico nella concessione di erogazioni o effettuazioni di pagamenti di qualsiasi natura;
- è fatto divieto di destinare somme ricevute da organismi pubblici nazionali o stranieri a titolo di contributo, sovvenzione o finanziamento a scopi diversi da quelli cui erano destinati;
- è vietato ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico funzionario, tali da influenzare le conclusioni dell'attività amministrativa;
- è vietato versare a chiunque, a qualsiasi titolo, somme o dare beni o altre utilità finalizzati a facilitare e/o rendere meno onerosa l'esecuzione e/o la gestione di contratti con la Pubblica Amministrazione rispetto agli obblighi in essi assunti;
- è vietato riconoscere compensi a consulenti, collaboratori o partner commerciali della Società che non trovino giustificazione nelle attività effettivamente prestate;
- è vietato alterare in qualsiasi modo i sistemi informatici e telematici della Società o manipolarne i dati.

A.5 Protocolli specifici di prevenzione

Per le operazioni riguardanti la **gestione dei rapporti con i rappresentanti della PA in occasione di accertamenti, ispezioni e verifiche (es. Agenzia delle Entrate; Guardia di Finanza), anche tramite consulenti esterni**, i protocolli prevedono che:

- nelle verifiche ispettive siano coinvolti almeno due rappresentanti;
- siano stabilite le modalità per dotare gli ispettori di idonee strutture (locali segregabili, accessi di rete, hardware) e le modalità con cui si rende disponibile agli stessi la documentazione aziendale;
- i soggetti responsabili della verifica informino l'OdV dell'inizio e della fine del procedimento e di qualsiasi criticità emersa durante il suo svolgimento, nonché gli comunichino:
  - ✓ i dati identificativi degli ispettori (nome ed ente di appartenenza);
  - ✓ la data e l'ora di arrivo degli ispettori;
  - ✓ la durata dell'ispezione;
  - ✓ l'oggetto della stessa;
  - ✓ l'esito della stessa;
  - ✓ l'eventuale verbale redatto dell'ente ispettivo;
  - ✓ l'elenco degli eventuali documenti consegnati;
- la documentazione sia conservata, ad opera dell'OdV, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- la documentazione sia conservata, ad opera del Responsabile della Funzione coinvolta, in un apposito archivio ben protetto, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

Per le operazioni riguardanti la **gestione dei rapporti con l'Autorità Giudiziaria, anche tramite consulenti esterni** e la **gestione del credito e del contenzioso contrattuale, anche tramite consulenti esterni**, i protocolli prevedono che:

Rapporti con l'Autorità Giudiziaria:

- sia sempre coinvolto l'Amministratore Unico, dotato dei poteri necessari per rappresentare la Società o per coordinare l'azione di eventuali professionisti esterni;
- l'Amministratore Unico informi l'OdV dell'inizio del procedimento giudiziario, delle risultanze delle varie fasi di giudizio, della conclusione del procedimento, nonché di qualsiasi criticità possa riscontrarsi *in itinere*;
- sia garantita la tracciabilità delle richiesta di informazioni ricevute nel corso del contenzioso e delle persone coinvolte, nonché del processo di valutazione e autorizzazione interna della documentazione consegnata nel corso del contenzioso.

Gestione del credito e del contenzioso:

- sia sempre coinvolto l'Amministratore Unico, dotato dei poteri necessari per rappresentare la Società o per coordinare l'azione di eventuali professionisti esterni;
- tutti gli atti, le richieste e le comunicazioni formali che hanno come controparte la PA siano gestiti e firmati solo da coloro che sono dotati di idonei poteri, in base alle procedure aziendali ed alle deleghe interne;
- sia garantita, in accordo con le procedure interne, la tracciabilità dei processi di monitoraggio del credito scaduto, di recupero crediti e di validazione interna e sottoscrizione di accordi transattivi.

Per le operazioni riguardanti la **gestione del contratto di servizio per la gestione del Sistema Informativo con il Comune di Parma**, i protocolli prevedono che:

- tutti gli atti, le richieste e le comunicazioni formali che hanno come destinatario il Comune di Parma devono essere gestiti e siglati solo dai soggetti dotati di idonei poteri, nel rispetto del contratto di servizio stipulato ("Contratto di servizio per la gestione del sistema informativo");
- l'Amministratore Unico autorizzi preventivamente l'utilizzo di dati e di informazioni riguardanti la Società e destinati ad atti, comunicazioni, attestazioni e richieste di qualunque natura inoltrate o aventi come destinatario la PA;
- l'Amministratore Unico verifichi che i documenti, le dichiarazioni e le informazioni trasmesse alla PA dalla Società siano complete e veritiere;
- in ogni trattativa in cui è coinvolta la PA, tutti i dipendenti operino nel rispetto delle leggi e dei regolamenti vigenti, nonché nel rispetto delle procedure aziendali in essere;
- la documentazione sia conservata, ad opera dei responsabili competenti, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- le somme ricevute a fronte delle prestazioni contrattuali rese nell'ambito del contratto di servizio ("Contratto di servizio per la gestione del sistema informativo") siano documentate e registrate in conformità ai principi di correttezza professionale e contabile.

Per le operazioni riguardanti la **richiesta di autorizzazioni, di concessioni e di certificazioni** e la **gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer**, i protocolli prevedono che:

- tutti gli atti, le richieste, e le comunicazioni formali che hanno come destinatario la PA siano sempre preventivamente autorizzati e successivamente sottoscritti dall'Amministratore Unico;
- il Responsabile interno per l'attuazione dell'operazione e/o il soggetto aziendale previsto dalle normative interne:

- identifichi gli strumenti più adeguati per garantire che i rapporti tenuti dalla propria Funzione con la PA siano sempre trasparenti, documentati e verificabili;
- autorizzi preventivamente l'utilizzo di dati e di informazioni riguardanti la Società destinati ad atti, comunicazioni, attestazioni e richieste di qualunque natura inoltrate o aventi come destinatario la PA;
- verifichi preventivamente che i documenti, le dichiarazioni e le informazioni trasmesse dalla Società alla PA siano complete e veritiere, e verifichi in particolare la loro conformità ai dati personali ed alle informazioni tenute presso i *data base* della Società.

Per le operazioni riguardanti la **richiesta, gestione, monitoraggio di contributi, esenzioni e agevolazioni fiscali, ecc., anche tramite consulenti esterni**, i protocolli prevedono che:

- il Responsabile interno per l'attuazione dell'operazione, verifichi che le dichiarazioni e la documentazione presentata al fine di ottenere il contributo o l'esenzione siano complete e rappresentino la reale situazione economica, patrimoniale e finanziaria della Società;
- le risorse finanziarie ottenute come contributo, esenzione o agevolazione fiscale siano destinate esclusivamente alle iniziative e al conseguimento delle finalità per le quali sono state richieste eottenute.

Per le operazioni riguardanti le **pubbliche relazioni che comportano rapporti con la PA (es. partecipazioni a convegni, meeting con enti pubblici)**, i protocolli prevedono che:

- possano intrattenere rapporti con la PA esclusivamente i soggetti preventivamente identificati e autorizzati dalla Società;
- sia prevista, per incontri particolarmente rilevanti, la partecipazione di almeno due rappresentanti della Società, scelti in base a valutazioni formalizzate che tengano in considerazione le finalità e l'oggetto dell'incontro;
- si provveda, per gli incontri rilevanti, alla rendicontazione dell'incontro attraverso la redazione di un verbale/memo, con l'indicazione del rappresentante della PA, dell'oggetto dell'incontro, degli esiti dello stesso e di ogni altra informazione rilevante;
- la documentazione sia conservata, ad opera del Responsabile della Funzione coinvolta, in un apposito archivio, con modalità tali da impedire la modifica successiva al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

Per le operazioni riguardanti la **gestione del processo di creazione, trattamento e archiviazione di documenti elettronici con valore probatorio**, i protocolli prevedono che:

- siano implementati controlli di sicurezza al fine di garantire la riservatezza dei dati interni alla rete e in transito su reti pubbliche;
- siano implementati meccanismi di tracciatura degli eventi di sicurezza sulle reti (ad es. accessi anomali per frequenza, modalità, temporalità);
- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa;
- tutti gli atti, le richieste, le comunicazioni formali siano gestiti e firmati solo da coloro che sono dotati di idonei poteri in base alle norme interne.

Per le operazioni riguardanti:

- **gestione delle risorse finanziarie (tramite Home banking);**
- **gestione degli approvvigionamenti (beni, servizi, appalti, software);**

- **conferimento e gestione delle consulenze;**
- **gestione del processo di assunzione e gestione del personale (tramite selezione pubblica);**
- **gestione delle note spese;**
- **gestione dei beni strumentali (es. PC, schede SIM).**

si applica quanto previsto al paragrafo 4 della presente Parte Speciale con riferimento alle corrispondenti attività sensibili.

SEZIONE B

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

(art. 24-*bis* del Decreto)

B.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte, in relazione alla Società sono considerati a rischio di commissione i seguenti delitti informatici:

a) **falsità in documenti informatici**, previsto dall'art. 491-*bis* c.p. e costituito dalle ipotesi di falsità, materiale o ideologica, commesse su atti pubblici, certificati, autorizzazioni, scritture private o atti privati, da parte di un rappresentante della Pubblica Amministrazione ovvero da un privato, qualora le stesse abbiano ad oggetto un "documento informatico avente efficacia probatoria", ossia un documento informatico munito quanto meno di firma elettronica semplice. Per "documento informatico" si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (tale delitto estende la penale perseguibilità dei reati previsti all'interno del Libro II, Titolo VII, Capo III del Codice Penale ai documenti informatici aventi efficacia probatoria);

b) **accesso abusivo ad un sistema informatico o telematico**, previsto dall'art. 615-*ter* c.p. e costituito dalla condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'ingresso in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo;

c) **detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**, previsto dall'art. 615-*quater* c.p. e costituito dalla condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno;

d) **diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**, previsto dall'art. 615-*quinquies* c.p., e che sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici;

e) **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**, previsto dall'art. 617-*quater* c.p., e che punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni;

f) **installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche**, previsto dall'art. 617-*quinquies* c.p., e che sanziona la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti fra più sistemi;

g) **danneggiamento di informazioni, dati e programmi informatici**, previsto dall'art. 635-*bis* c.p. e costituito dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato;

h) **danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità**, previsto dall'art. 635-*ter* c.p. e costituito dalla condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto costituisca più grave reato;

i) **danneggiamento di sistemi informatici o telematici**, previsto dall'art. 635-*quater* c.p. e costituito dalla condotta di chi, mediante le condotte di cui all'art. 635-*bis* c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento salvo che il fatto costituisca più grave reato;

j) **danneggiamento di sistemi informatici o telematici di pubblica utilità**, previsto dall'art. 635-*quinquies* c.p. e costituito dalla condotta descritta al precedente articolo 635-*quater* c.p., qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento;

k) **frode informatica del soggetto che presta servizi di certificazione di firma elettronica**, previsto dall'art. 640-*quinquies* c.p. e costituito dalla condotta del soggetto che presta servizi di certificazione di firma elettronica il quale, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

B.2 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei delitti informatici e trattamento illecito di dati previsti dall'art. 24-*bis* del Decreto:

- ✓ Gestione del processo di creazione, trattamento e archiviazione di documenti elettronici con valore probatorio;
- ✓ Gestione dei profili utente e del processo di autenticazione;
- ✓ Gestione e protezione della postazione di lavoro;
- ✓ Accessi da e verso l'esterno;
- ✓ Gestione e protezione delle reti;
- ✓ Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD);
- ✓ Sicurezza fisica;
- ✓ Produzione e/o vendita di programmi informatici e di servizi di installazione e manutenzione di hardware, software e reti;
- ✓ Gestione e/o manutenzione per conto proprio e/o di terzi di apparecchiature, dispositivi e programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti.

B.3 Protocolli generali di prevenzione

Al fine di prevenire la commissione dei reati 231 nell'ambito delle aree, attività e operazioni a rischio precedentemente identificate, la Società elabora e adotta procedure che devono, in ogni caso, rispettare i seguenti principi generali:

- la formazione e l'attuazione delle decisioni dell'Amministratore siano disciplinate dai principi e dalle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, dello Statuto, del Modello, delle istruzioni e raccomandazioni delle Autorità di Vigilanza e Controllo.
- vi sia l'obbligo per l'Amministratore di comunicare tempestivamente al Collegio Sindacale e all'Organismo di vigilanza- ODV, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative alle cariche direttamente assunte, alle partecipazioni di cui sono titolari, direttamente o indirettamente, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia, possono lasciare ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.;
- siano tempestivamente e correttamente effettuate, in modo veritiero e completo, le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità o Organi, anche Societari, di Vigilanza o Controllo, del mercato o dei soci;
- sia prestata completa e immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed esaustivamente la documentazione e le informazioni richieste;

- sia prevista l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione al cliente, controparte o ente interessati, con precisa individuazione del beneficiario e della causale dell'operazione, con modalità tali da consentire l'individuazione del soggetto che ha disposto l'operazione o l'ha effettuata; il sistema deve prevedere l'impossibilità di modificare le registrazioni;
- nello svolgimento delle attività, i Destinatari sono tenuti ad attenersi, oltre che alle disposizioni contenute nei capitoli successivi, anche a quanto contenuto nei "Regolamenti", nei "Manuali di processo", nelle "Disposizioni operative", nel "Codice Etico" e nelle procedure relative alle aree di attività a rischio.

B.4 Protocolli specifici di prevenzione

Qui di seguito sono elencati gli standard di controllo individuati per le specifiche attività sensibili rilevate in ambito di sicurezza informatica.

Politiche di sicurezza

Policy: sono formalizzate le policy in materia di sicurezza del sistema informativo, finalizzate a fornire le direttive ed il supporto per la gestione della sicurezza delle informazioni in accordo con le necessità di business, la normativa e gli aspetti regolatori. Le policy chiariscono gli obiettivi, i processi ed i controlli necessari per la gestione della sicurezza informatica.

Tali policy, approvate dall'Amministratore Unico, prevedono tra l'altro:

- le modalità di diffusione e di comunicazione delle stesse anche a terzi;
- le modalità di riesame delle stesse, periodico o a seguito di cambiamenti significativi.

Organizzazione della sicurezza per gli utenti interni

Regolamento: è adottato e attuato un regolamento che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.

Organizzazione della sicurezza per gli utenti esterni.

- Procedura: è adottata e attuata una procedura che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.
- Clausole contrattuali: i contratti con i fornitori devono prevedere clausole specifiche per la gestione della sicurezza.

Classificazione e controllo dei beni

Procedura: sono adottate e attuate procedure che definiscono i ruoli e le responsabilità per l'identificazione e la classificazione degli assets aziendali (ivi inclusi dati e informazioni). Tali procedure consentono di individuare la criticità degli assets in termini di sicurezza informatica e sono finalizzate alla definizione degli opportuni meccanismi di protezione ed alla coerente gestione dei flussi di comunicazioni.

Sicurezza fisica e ambientale

Misure di sicurezza fisica: sono adottate e attuate le misure di sicurezza finalizzate a prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

Gestione delle comunicazioni e dell'operatività

- Procedura: sono adottate e attuate una serie di procedure che assicurano la correttezza e la sicurezza dell'operatività dei sistemi informativi. In particolare, tali procedure disciplinano:
  - il corretto e sicuro funzionamento degli elaboratori di informazioni;
  - la protezione da software pericoloso;
  - il backup di informazioni e software;
  - la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
  - gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
  - una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
  - il controllo sui cambiamenti agli elaboratori e ai sistemi;
  - la gestione di dispositivi rimovibili.

- Clausole contrattuali: la correttezza e la sicurezza dell'operatività dei sistemi informativi nei rapporti con i clienti è garantita attraverso l'inserimento di specifiche clausole contrattuali che definiscono le regole operative.

Controllo degli accessi

- Procedure: sono adottate e attuate specifiche procedure che disciplinano gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi ed alle applicazioni.
  In particolare, tali procedure prevedono:
  - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  - le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
  - una procedura di registrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
  - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
  - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
  - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
  - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
  - la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati.

- Clausole contrattuali: gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi e alle applicazioni nei rapporti con i clienti è garantita attraverso l'inserimento di specifiche clausole contrattuali che ne definiscono le modalità.

Gestione degli incidenti e dei problemi di sicurezza informatica

- Procedure: sono adottate e attuate specifiche procedure che definiscono le modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tali procedure prevedono:
  - appropriati canali gestionali per la comunicazione degli incidenti e problemi;
  - l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della "root cause";
  - la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
  - l'analisi di report e trend sugli incidenti e sui problemi e l'individuazione di azioni preventive;
  - appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
  - l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
  - l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
  - la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi "workaround" e le soluzioni definitive, identificate o implementate;
  - la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti e alla sicurezza informativa.

- Clausole contrattuali: la gestione degli incidenti e dei problemi di sicurezza nei rapporti con i clienti è garantita attraverso l'inserimento di specifiche clausole contrattuali che ne definiscono le modalità.

Audit

- Procedure: sono adottate specifiche procedure che disciplinano i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.
- Audit: vengono svolte attività di audit atte a verificare l'applicazione delle misure di sicurezza previste, sia nelle configurazioni dei sistema che nei singoli processi organizzativi.

Risorse umane e sicurezza

Procedure: sono adottate e attuate procedure, in conformità con quanto previsto dal Decreto Legge 31 maggio 2010 n. 78, convertito in Legge 122/2010 in materia di politiche del personale, e in base a quanto indicato all'interno del Regolamento Gruppo Comune di Parma, che prevedono:

- la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
- specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
- l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, strumenti di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi

Procedura: sono adottate e attuate procedure che definiscono:

- l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- la confidenzialità, autenticità e integrità delle informazioni;
- la sicurezza nel processo di sviluppo dei sistemi informativi.

B.5 Delitti informatici e Codice della Privacy

La compliance alle disposizioni contenute nel Codice della Privacy sul trattamento di dati personali, mediante l'impiego di risorse informatiche rappresenta un valido strumento per impostare gli accorgimenti organizzativi utili alla prevenzione dei reati informatici. La mancanza di adeguate misure di protezione dei sistemi, degli archivi e dei dati potrebbe tradursi infatti, in accesso non autorizzato, in comunicazione e diffusione improprie, alterazione, perdita temporanea o definitiva di informazioni ecc. e creare i presupposti non solo per la violazione alla disciplina sulla privacy (trattamento illecito dei dati), ma anche di reati informatici.

La Società, pertanto, ispirandosi ai principi di necessità, correttezza e segretezza enunciati nel Codice della Privacy, per contrastare i rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto del trattamento; di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta, adotta un adeguato sistema di sicurezza basato su:

- regolamentazione dei comportamenti
- formazione obbligatoria
- controllo del personale interno ed esterno

Ruoli e responsabilità

L'Amministratore Unico di IT.CITY ha nominato il Responsabile del trattamento dati ai sensi del d. lgs. 196/03, il quale, al fine di assicurare la funzionalità e il corretto impiego da parte degli utenti delle risorse informatiche:

- valuta il grado di rischio di incidenti di sicurezza informatica da parte del personale o di soggetti esterni (consulenti, agenti ecc...);
- supporta il Titolare nel definire le modalità operative di trattamento;
- adotta idonee misure di sicurezza, di tipo organizzativo e tecnologico per garantire la disponibilità e l'integrità di sistemi informativi e di dati e per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- supporta il Titolare nell'elaborazione un Regolamento Interno relativo a:
  - utilizzo del personal computer,
  - utilizzo della rete interna aziendale,
  - assegnazione e gestione delle password,
  - utilizzo del servizio di posta elettronica,
  - accesso a particolari informazioni,

- prescrizioni sulla sicurezza dei dati e dei sistemi,
- utilizzo e conservazione dei supporti rimovibili,
- uso della rete internet e dei relativi servizi,
- policy in materia di privacy;

- osserva e garantisce il rispetto delle disposizioni contenute nel Regolamento;
- aggiorna il Regolamento aziendale al verificarsi di eventi tali da pregiudicarne l'efficacia (modifiche legislative e regolamentari, mutamenti della struttura aziendale e delle funzioni coinvolte nello svolgimento dell'attività ecc...);
- denuncia eventuali accessi al sistema informatico aziendale da parte di hackers;
- rende consapevoli i lavoratori delle potenzialità degli strumenti e dei programmi elettronici implementati dall'azienda, attraverso un'attività di formazione obbligatoria che illustra:
  - i rischi che incombono sui dati;
  - le misure disponibili per prevenire eventi dannosi;
  - le responsabilità che ne derivano.

SEZIONE C

DELITTI DI CRIMINALITÀ ORGANIZZATA E REATI TRASNAZIONALI

(art. 24-*ter* del Decreto e art. 10 L. 146/2006)

C.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerati applicabili alla Società i seguenti delitti di criminalità organizzata e reati transnazionali:

a) **associazione per delinquere**, previsto dall'art. 416 c.p. e che punisce coloro che promuovono o costituiscono od organizzano un'associazione di tre o più persone allo scopo di commettere più delitti, nonché coloro che vi partecipano;

b) **associazione di tipo mafioso anche straniera**, previsto dall'art. 416-*bis* c.p. e che punisce chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, nonché coloro che la promuovono, dirigono o organizzano. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali. L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito. Le disposizioni dell'art. 416-*bis* c.p. si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso;

c) **delitti commessi avvalendosi delle condizioni previste dall'articolo 416-*bis* c.p., ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo**;

d) **scambio elettorale politico-mafioso**, previsto dall'art. 416-ter c.p. e costituito dalla condotta di chiunque accetta la promessa di procurare voti mediante le modalità di cui al terzo comma dell´articolo 416-bis in cambio dell´erogazione o della promessa di erogazione di denaro o di altra utilità.

e) **induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria**, previsto dall' art. 377-*bis* c.p., e costituito dalla condotta di chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla Autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere. Tale reato, ai sensi di quanto previsto dall'art. 10 della legge n. 146 del 2006, potrà essere considerato reato-presupposto laddove risultino soddisfatte le condizioni di cui all'art. 3 della medesima legge, contenente la "Definizione di reato transnazionale".

f) **favoreggiamento personale,** previsto dall'art. 378 c.p. e costituito dalla condotta di chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce la pena di morte o l'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'autorità, o a sottrarsi alle ricerche di questa. Tale reato, ai sensi di quanto previsto dall'art. 10 della legge n. 146 del 2006, potrà essere considerato reato-presupposto laddove risultino soddisfatte le condizioni di cui all'art. 3 della medesima legge, contenente la "Definizione di reato transnazionale".

C.2 Attività sensibili

Salvo quanto previsto dalla Sezione I alla quale si rimanda con riferimento alla fattispecie di cui alla lettera d) del precedente paragrafo, i delitti di cui all'art. 24-*ter* del Decreto e di cui all'art. 10, L. 146/2006 non sembrano poter essere ricollegati a specifiche attività svolte in concreto dalla Società. Inoltre, va evidenziato che:

- tali delitti hanno natura, per ampia parte, di reati associativi (associazione per delinquere, associazione di tipo mafioso anche straniera) o fortemente collegati a reati associativi (scambio elettorale politico-mafioso, delitti commessi avvalendosi delle modalità di cui all'art. 416-*bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso), che puniscono perciò anche solo l'accordo di più persone volto alla commissione di un numero e di un tipo indeterminato di delitti;
- i reati associativi, essendo per definizione costituiti dall'accordo volto alla commissione di qualunque delitto, estendono il novero dei reati presupposto ad un numero indeterminato di figure criminose, per cui qualsiasi attività svolta dalla Società potrebbe comportare la commissione di un delitto – e la conseguente responsabilità *ex* D.Lgs. 231/2001 – "tramite" un'associazione per delinquere.

Sebbene, però, tali reati risultino essere, come detto sin qui, non riconducibili a specifiche attività concretamente svolte dalla Società – e, quindi, alle relative procedure operative – gli stessi possono essere astrattamente commessi tanto da soggetti apicali che da subordinati. Con riferimento a tale aspetto, assume rilevanza il sistema di prevenzione già in essere nella Società.

Si è infatti ritenuto che, per la prevenzione di detti reati, possano svolgere un'adeguata funzione preventiva i presidi di *corporate governance* già in essere, nonché i principi presenti nel Codice Etico, che costituiscono lo strumento più adeguato per reati come l'associazione per delinquere di cui all'art. 416 c.p., per l'impossibilità di inquadrare all'interno di uno specifico sistema di controlli il numero pressoché infinito di comportamenti che potrebbero essere commessi mediante il vincolo associativo.

Nondimeno, la Società ha in ogni caso individuato una serie di attività in cui soggetti riconducibili ad associazioni criminose, o che comunque svolgono attività illecite, possono entrare in contatto e gestire attività di impresa con la Società stessa. In particolare, sono state individuate le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati delitti di criminalità organizzata previsti dall'art. 24-*ter* del Decreto e reati transnazionali previsti dall'art. 10, L. 146/2006:

- ✓ Gestione delle risorse finanziarie (tramite Home banking);
- ✓ Gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer;
- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Gestione del processo di assunzione e gestione del personale (tramite selezione pubblica).

C.3 Protocolli specifici di prevenzione

Per le operazioni riguardanti la **gestione degli approvvigionamenti (beni, servizi, appalti, software)** si applica quanto previsto al paragrafo 4 della presente Parte Speciale con riferimento alla corrispondente attività sensibile. Inoltre, i protocolli prevedono che:

- per le fatture ricevute dalla Società a fronte dell'acquisto di beni e servizi sia verificata l'effettiva corrispondenza delle stesse – con riferimento sia all'esistenza della transazione, sia all'importo della stessa come indicato in fattura – ai contratti, agli ordini di acquisto o alle conferme d'ordine in essere presso la Società.

Per le operazioni riguardanti la **gestione delle risorse finanziarie (tramite Home banking)** e la **gestione del processo di assunzione e gestione del personale (tramite selezione pubblica)** si applica quanto previsto al paragrafo 4 della presente Parte Speciale con riferimento alle corrispondenti attività sensibili.

Per le operazioni riguardanti la **gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer,** si applica quanto previsto al paragrafo A.5 della presente Parte Speciale con riferimento alla corrispondente attività sensibile.

SEZIONE D

DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

(art. 25-*bis.1* del Decreto)

D.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerati configurabili rispetto alla Società i seguenti delitti contro l'industria e il commercio:

a) **turbata libertà dell'industria o del commercio**, previsto dall'art. 513 c.p e che punisce chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio.

b) **illecita concorrenza con minaccia o violenza**, previsto dall'art. 513-bis c.p. e che punisce chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia.

c) **frode nell'esercizio del commercio**, previsto dall'art. 515 c.p. e che punisce chiunque, nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.

D.2 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati delitti contro l'industria e il commercio previsti dall'art. 25-*bis*.1 del Decreto:

✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software).

D.3 Protocolli specifici di prevenzione

Per le operazioni riguardanti la **gestione degli approvvigionamenti (beni, servizi, appalti, software)** si applica quanto previsto al paragrafo 4 della presente Parte Speciale con riferimento alla corrispondente attività sensibile.

SEZIONE E

REATI SOCIETARI E CORRUZIONE TRA PRIVATI

(art. 25-*ter* del Decreto)

E.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerati configurabili rispetto alla Società i seguenti reati societari:

a) **false comunicazioni sociali**, previste dall'art. 2621 c.c. e costituite dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore;

b) **false comunicazioni sociali di lieve entità**, previste dall'art. 2621-*bis* c.c. e costituita dalla condotta di chi commette i fatti previsti dall'art. 2621 c.c. in misura lieve, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta;

c) **impedito controllo**, previsto dall'art. 2625 c.c. e costituito dalla condotta degli amministratori i quali, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali;

d) **indebita restituzione dei conferimenti**, previsto dall'art. 2626 c.c. e costituito dalla condotta degli amministratori i quali, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli;

e) **illegale ripartizione degli utili e delle riserve**, previsto dall'art. 2627 c.c. e costituito dalla condotta degli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite;

f) **illecite operazioni sulle azioni o quote sociali o della società controllante**, previsto dall'art. 2628 c.c. e costituito dalla condotta degli amministratori i quali, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge; ovvero dagli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge;

g) **operazioni in pregiudizio dei creditori**, previsto dall'art. 2629 c.c. e costituito dalla condotta degli amministratori i quali, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori;

h) **formazione fittizia del capitale**, previsto dall'art. 2632 c.c. e costituito dalla condotta degli amministratori e dei soci conferenti i quali, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione;

i) **corruzione tra privati**, previsto dall'art. 2635, comma 3, c.c. e costituito dalla condotta di colui che dà o promette denaro o altra utilità agli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, nonché a coloro che sono sottoposti alla direzione o alla vigilanza di detti soggetti, affinché, per sé o per altri, compiano o omettano atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società;

j) **aggiotaggio**, previsto dall'art. 2637 c.c. e costituito dalla condotta chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari;

k) **ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza**, previsto dall'art. 2638 c.c. e costituito dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori di società o enti e degli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi; ovvero dal fatto commesso dagli amministratori, dai direttori generali, dai sindaci e dai liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

E.2 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati reati societari previsti dall'art. 25-*ter* del Decreto:

- ✓ Richiesta di autorizzazioni, di concessioni e di certificazioni;
- ✓ Gestione delle risorse finanziarie (tramite Home banking);
- ✓ Gestione del credito e del contenzioso contrattuale, anche tramite consulenti esterni;
- ✓ Valutazioni e stime di poste soggettive di bilancio; rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti di impresa, anche tramite consulenti esterni;
- ✓ Gestione dei rapporti con il socio unico ed il Collegio Sindacale;
- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Conferimento e gestione delle consulenze;
- ✓ Gestione del processo di assunzione e gestione del personale (tramite selezione pubblica);
- ✓ Gestione delle note spese;
- ✓ Gestione dei beni strumentali (es. PC, schede SIM).

E.3 Protocolli specifici di prevenzione

Per le operazioni riguardanti le **valutazioni e stime di poste soggettive di bilancio; rilevazione, registrazione e rappresentazione dell'attività d'impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti d'impresa, anche tramite consulenti esterni**, i protocolli prevedono che:

- tutte le operazioni di rilevazione e registrazione delle attività di impresa siano effettuate con correttezza e nel rispetto dei principi di veridicità e completezza;
- i responsabili delle diverse funzioni aziendali forniscano le informazioni loro richieste in modo tempestivo e attestando, ove possibile, la completezza e la veridicità delle informazioni;

- qualora utile per la comprensione dell'informazione, i relativi Responsabili indichino i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, e, ove possibile, ne alleghino copia;
- la rilevazione, la trasmissione e l'aggregazione delle informazioni contabili finalizzate alla predisposizione delle comunicazioni sociali avvenga esclusivamente tramite modalità che possano garantire la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei soggetti che inseriscono i dati nel sistema; siano identificati i profili di accesso a tale sistema garantendo la separazione delle funzioni e la coerenza dei livelli autorizzativi;
- eventuali modifiche alle poste di bilancio o ai criteri di contabilizzazione delle stesse siano preventivamente autorizzate;
- la richiesta da parte di chiunque di ingiustificate variazioni dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure operative della Società, sia oggetto di immediata comunicazione all'Organismo di Vigilanza;
- le bozze del bilancio e degli altri documenti contabili siano messi a disposizione dell'Amministratore Unico con ragionevole anticipo rispetto all'approvazione del bilancio.

Per le operazioni riguardanti la **gestione dei rapporti con il socio unico ed il Collegio Sindacale,** i protocolli prevedono che:

- per ciascuna Funzione sia 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 Socio e dal Collegio Sindacale, siano documentate e conservate;
- tutti i documenti relativi ad operazioni all'ordine del giorno delle riunioni dell'Assemblea o dell'Amministratore Unico o, comunque, relativi a operazioni sulle quali il Collegio Sindacale debba esprimere un parere, siano comunicati e messi a disposizione con ragionevole anticipo;
- sia garantito al Socio e al Collegio Sindacale il libero accesso alla contabilità aziendale e a quanto altro richiesto per un corretto svolgimento dell'incarico.

Per le operazioni riguardanti la **richiesta di autorizzazioni, di concessioni e di certificazioni** e la **gestione del credito e del contenzioso contrattuale, anche tramite consulenti esterni,** si applica quanto previsto al paragrafo A.5 della presente Parte Speciale con riferimento alle corrispondenti attività sensibili.

Per le operazioni riguardanti:

- **gestione delle risorse finanziarie (tramite Home banking);**
- **gestione degli approvvigionamenti (beni, servizi, appalti, software);**
- **conferimento e gestione delle consulenze;**
- **gestione del processo di assunzione e gestione del personale (tramite selezione pubblica);**
- **gestione delle note spese;**
- **gestione dei beni strumentali (es. PC, schede SIM).**

si applica quanto previsto al paragrafo 4 della presente Parte Speciale con riferimento alle corrispondenti attività sensibili.

SEZIONE F

REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME PER VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI SALUTE E SICUREZZA DEI LUOGHI DI LAVORO

(art. 25-*septies* del Decreto)

F.1 Premessa

Sulla base delle analisi condotte sono considerati applicabili alla Società i delitti di omicidio colposo e di lesioni personali colpose gravi o gravissime, commessi con violazione della normativa antinfortunistica e sulla tutela della salute e della sicurezza nei luoghi di lavoro.

Gli artt. 589 e 590, comma 3 c.p., richiamati dall'art. 25-septies del Decreto, sanzionano chiunque, per colpa, cagioni rispettivamente la morte di una persona ovvero le arrechi lesioni personali gravi o gravissime5.

La norma sanziona chiunque, per colpa, comporti la morte di una persona ovvero le arrechi lesioni personali.

Per "*lesione*" si intende l'insieme degli effetti patologici costituenti malattia, ossia quelle alterazioni organiche e funzionali conseguenti al verificarsi di una condotta violenta: la lesione è grave se la malattia ha messo in pericolo la vita della vittima, ha determinato un periodo di convalescenza superiore ai quaranta giorni, ovvero ha comportato l'indebolimento permanente della potenzialità funzionale di un senso, come l'udito, o di un organo, ad esempio l'apparato dentale. È gravissima se la condotta ha determinato una malattia probabilmente insanabile (con effetti permanenti non curabili) oppure ha cagionato la perdita totale di un senso, di un arto, della capacità di parlare correttamente o di procreare, la perdita dell'uso di un organo ovvero ha deformato o sfregiato il volto della vittima.

Si configura, invece, un "*omicidio*" nel momento in cui una condotta violenta produce la morte di un individuo, ossia la definitiva perdita di vitalità dello stesso.

L'evento dannoso, sia esso rappresentato dalla lesione grave o gravissima o dalla morte, può essere perpetrato tramite un *comportamento attivo* (l'agente pone in essere una condotta con cui lede l'integrità di un altro individuo), ovvero mediante un *atteggiamento omissivo* (l'agente semplicemente non interviene a impedire l'evento dannoso). Di norma, si ravviserà una condotta attiva nel lavoratore subordinato che svolge direttamente mansioni operative e che materialmente danneggia altri, mentre la condotta omissiva sarà usualmente ravvisabile nel personale apicale che non ottempera agli obblighi di vigilanza e controllo e in tal modo non interviene ad impedire l'evento da altri causato.

Con riferimento a quanto evidenziato poc'anzi in merito all'atteggiamento omissivo, si specifica che un soggetto risponde della propria condotta colposa omissiva, lesiva della vita o dell'incolumità fisica di una persona, soltanto se riveste nei confronti della vittima una *posizione di garanzia*, che può avere origine da un contratto oppure dalla volontà unilaterale dell'agente. Le norme individuano nel *datore di lavoro*[6] il garante "*dell'integrità fisica e della personalità morale dei prestatori di lavoro*" e la sua posizione di garanzia è comunque trasferibile ad altri soggetti, a patto che la relativa delega sia sufficientemente specifica, predisposta mediante atto scritto e idonea

---

[5] Art. 589 c.p. Omicidio colposo: «Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme [...] per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a cinque anni. [...] Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici».

Art. 590 c.p. Lesioni personali colpose: «Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a € 309. Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da € 123 a € 619; se è gravissima, della reclusione da tre mesi a due anni o della multa da € 309 a € 1.239. Se i fatti di cui al secondo comma sono commessi con violazione delle norme [...] per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da € 500 a € 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. [...] Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque. Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale».

[6] Soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa (art. 2 comma 1 D.Lgs. 81/08).

a trasferire tutti i poteri autoritativi e decisori necessari per tutelare l'incolumità dei lavoratori subordinati. Il prescelto a ricoprire l'incarico deve essere persona capace e competente per la materia oggetto del trasferimento di responsabilità.

In base alle novità normative introdotte dal legislatore, la condotta lesiva dell'agente deve essere necessariamente *aggravata*, ossia conseguire alla violazione di norme antinfortunistiche e concernenti la tutela dell'igiene e la salute sul lavoro. Ai fini dell'implementazione del Modello è necessario comunque considerare che:

- il rispetto degli standard minimi di sicurezza previsti dalla normativa specifica di settore non esaurisce l'obbligo di diligenza complessivamente richiesto (aspetto relativo alla colpa specifica);
- è necessario garantire l'adozione di standard di sicurezza tali da minimizzare (e, se possibile, eliminare) ogni rischio di infortunio e malattia, anche in base dalla miglior tecnica e scienza conosciute, secondo le particolarità del lavoro (aspetto relativo alla colpa generica);
- ai fini del Modello, non esclude tutte le responsabilità in capo all'ente il comportamento del lavoratore infortunato che abbia dato occasione all'evento, quando quest'ultimo sia da ricondurre, comunque, alla mancanza o insufficienza delle cautele che, se adottate, avrebbero neutralizzato il rischio sotteso a un siffatto comportamento. L'obbligo di prevenzione è escluso solo in presenza di comportamenti del lavoratore che presentino il carattere dell'eccezionalità, dell'abnormità, dell'esorbitanza rispetto al procedimento lavorativo, alle direttive organizzative ricevute e alla comune prudenza.

Sotto il profilo dei soggetti tutelati, le norme antinfortunistiche non tutelano solo i dipendenti, ma tutte le persone che legittimamente si introducono nei locali adibiti allo svolgimento della prestazione lavorativa.

Per quanto concerne i soggetti attivi, possono commettere queste tipologie di reato coloro che, in ragione della loro mansione, svolgono attività sensibili in materia. Ad esempio:

- il lavoratore che, attraverso le proprie azioni e/o omissioni, può pregiudicare la propria ed altrui salute e sicurezza;
- il dirigente ed il preposto, ai quali possono competere, tra gli altri, i compiti di coordinamento e supervisione delle attività, di formazione e di informazione;
- il datore di lavoro quale principale attore nell'ambito della prevenzione e protezione;
- il progettista, al quale compete il rispetto dei principi di prevenzione in materia di salute e sicurezza sul lavoro, sin dal momento delle proprie scelte progettuali e tecniche;
- il fabbricante, l'installatore ed il manutentore che, nell'ambito delle rispettive competenze, devono assicurare il rispetto delle norme tecniche applicabili;
- il committente, al quale competono, secondo le modalità definite dalla normativa, la gestione ed il controllo dei lavori affidati in appalto.

F.2 Attività sensibili

F.2.1 Premessa

Per definire preliminarmente le attività sensibili, ai sensi del D.Lgs. 231/2001, occorre considerare le attività entro le quali si possono verificare gli infortuni e le malattie professionali e quelle nell'ambito delle quali può essere commesso, da parte di membri dell'organizzazione, il reato per violazione colposa della normativa e delle misure di prevenzione esistenti a tutela della salute, dell'igiene e della sicurezza sui luoghi di lavoro. A tale fine, la Società ha reputato strategico trarre spunto da due importanti strumenti di controllo e di gestione:

- la valutazione di rischi prevista dalla vigente normativa in materia di tutela della salute e della sicurezza;
- la Norma BS OHSAS 18001:2007.

Attraverso la Valutazione dei rischi si sono individuate le condizioni ove, ragionevolmente, è possibile si manifestino degli eventi lesivi.

F.2.2 Le attività sensibili

Le attività che la Società ha individuato al proprio interno come sensibili, nell'ambito dei reati di omicidio colposo e di lesioni personali colpose gravi o gravissime, riconducibili alla violazione della normativa di tutela della salute e della sicurezza nei luoghi di lavoro, sono di seguito indicate:

(i) **attività a rischio di infortunio e malattia professionale**, mutuate dal documento di valutazione dei rischi aziendali di cui all'art. 28 del D. Lgs. 9 aprile 2008 n. 81, redatto dal datore di lavoro ed intese come le attività dove potenzialmente si possono materializzare gli infortuni e le malattie professionali;

(ii) **attività a rischio di reato**, intese come le attività che possono potenzialmente originare i reati di cui all'art. 25-septies del Decreto, in quanto una loro omissione o un'inefficace attuazione potrebbero integrare una responsabilità colposa della Società, e che costituiscono l'elemento centrale per adottare ed efficacemente attuare un sistema idoneo all'adempimento di tutti gli obblighi giuridici richiesti dalla normativa vigente sulla salute e sicurezza sul lavoro. Attraverso un'attività di control and risk self assessment, che costituisce parte integrante del Modello, la Società ha individuato le attività a rischio di reato e valutato per esse l'eventuale devianza dal sistema di gestione nella conduzione delle stesse.

Attività a rischio di infortunio e malattia professionale

Attraverso attente analisi che interessano sia aspetti strutturali sia aspetti organizzativi, sono individuati i rischi per la sicurezza e la salute dei lavoratori.

Gli esiti di tali analisi, che consentono l'individuazione dei rischi che possono dare origine ad infortuni e malattie professionali, sono contenuti negli specifici documenti di valutazione dei rischi ove sono altresì indicate le misure di tutela atte alla loro eliminazione ovvero al loro contenimento. Le attività entro le quali possono verificarsi infortuni o malattie professionali sono quindi desunte dagli specifici documenti di valutazione dei rischi a cui questo elaborato rimanda.

I documenti di valutazione dei rischi sono costantemente aggiornati, in relazione a nuove ed eventuali esigenze di prevenzione, secondo le procedure previste dal presente Modello.

Sulla base di quanto emerge dalla valutazione dei rischi effettuata ed alla luce dei controlli attualmente esistenti, sono stati individuati i principi di comportamento e i protocolli di prevenzione.

Attività a rischio di reato

Le attività che possono potenzialmente originare i reati di cui all'art. 25-*septies* del Decreto, in quanto una loro omissione o un'inefficace attuazione potrebbe integrare una responsabilità colposa della Società, sono riportate di seguito. La loro individuazione è stata condotta in accordo con quanto previsto dall'art. 30, D. Lgs. 81/2008 e considerando i requisiti previsti dalla Norma BS OHSAS 18001:2007 cui il Modello è ispirato.

- ✓ Individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali;
- ✓ Definizione delle risorse, dei ruoli e delle responsabilità per assicurare le attività finalizzate all'attuazione delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- ✓ Valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti;
- ✓ Individuazione e gestione delle misure di protezione collettiva e/o individuale atte a contenere o ad eliminare i rischi;
- ✓ Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso;
- ✓ Gestione degli approvvigionamenti e degli acquisti (incluso l'acquisizione della documentazione e delle certificazioni obbligatorie per legge);
- ✓ Attività di sorveglianza sanitaria;
- ✓ Competenza, informazione, formazione e consapevolezza dei lavoratori;
- ✓ Attività di comunicazione, partecipazione e consultazione, gestione delle riunioni periodiche di sicurezza, consultazione dei rappresentanti dei lavoratori per la sicurezza;
- ✓ Gestione della documentazione e dei sistemi di registrazione al fine di garantire la tracciabilità delle attività.

F.3 Principi generali di comportamento

Il Modello non intende sostituirsi alle prerogative e responsabilità di legge disciplinate in capo ai soggetti individuati dal D. Lgs. 81/2008 e dalla normativa ulteriormente applicabile nei casi di specie. Costituisce, invece, un presidio ulteriore di controllo e verifica dell'esistenza, efficacia ed adeguatezza della struttura e organizzazione posta in essere in ossequio alla normativa speciale vigente in materia di antinfortunistica, tutela della sicurezza e della salute nei luoghi di lavoro.

Tutti i Destinatari del Modello, come individuati nel Paragrafo 3.6 della Parte Generale, adottano regole di condotta conformi ai principi contenuti nel Codice Etico della Società, nella normativa antinfortunistica nonché negli Strumenti di attuazione del Modello, al fine di prevenire il verificarsi dei reati di omicidio e lesioni colposi, sopra identificati.

In particolare, costituiscono presupposto e parte integrante dei protocolli di prevenzione i principi di comportamento individuati nel Codice Etico, che qui si intende integralmente richiamato, la documentazione relativa alla tutela ed alla sicurezza dei luoghi di lavoro (ivi compresi il Documento di Valutazione dei Rischi nonché le procedure di gestione delle emergenze).

Presupposti essenziali del Modello al fine della prevenzione degli infortuni sui luoghi di lavoro sono il rispetto di alcuni principi e la tenuta di determinati comportamenti da parte dei lavoratori della Società, nonché dagli eventuali soggetti esterni che si trovino legittimamente presso i locali della Società stessa. In particolare, ciascun lavoratore e ciascun soggetto che si trovi legittimamente presso la Società, ovvero la cui attività ricada sotto la responsabilità della stessa, dovrà:

a) conformemente alla propria formazione ed esperienza, nonché alle istruzioni e ai mezzi forniti ovvero predisposti dal datore di lavoro, non adottare comportamenti imprudenti quanto alla salvaguardia della propria salute e della propria sicurezza;
b) rispettare la normativa e le procedure aziendali interne al fine della protezione collettiva ed individuale, esercitando in particolare ogni opportuno controllo ed attività idonee a salvaguardare la salute e la sicurezza dei collaboratori esterni e/o di persone estranee, eventualmente presenti sul luogo di lavoro;
c) utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze ed i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
d) utilizzare in modo appropriato i dispositivi di protezione messi a disposizione;
e) segnalare immediatamente a chi di dovere (in ragione delle responsabilità attribuite) le anomalie dei mezzi e dei dispositivi di cui ai punti precedenti, nonché le altre eventuali condizioni di pericolo di cui si viene a conoscenza;
f) intervenire direttamente, a fronte di un pericolo rilevato e nei soli casi di urgenza, compatibilmente con le proprie competenze e possibilità;
g) sottoporsi ai controlli sanitari previsti;
h) sottoporsi agli interventi formativi previsti;
i) contribuire all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

A questi fini è fatto divieto di:

a) rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
b) compiere di propria iniziativa operazioni o manovre che non sono di propria competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori.

F.4 Protocolli specifici di prevenzione

Il Documento di Valutazione dei Rischi (di seguito anche DVR) indica specifiche misure di prevenzione degli infortuni e delle malattie professionali a cui si rinvia direttamente. Si precisa che, ai fini del mantenimento del modello di organizzazione, gestione e controllo, si rende necessario dare evidenza di quanto attuato; ciò avviene attraverso l'adozione di sistemi di registrazione appropriati. È altresì rilevante garantire la disponibilità e l'aggiornamento della documentazione sia di origine interna, sia di origine esterna (es. documentazione relativa a prodotti e sostanze), anche attraverso un controllo periodico della conformità alla normativa applicabile.

Procedure e protocolli di prevenzione sono reperibili nella rete intranet aziendale.

Ai fini dell'adozione e dell'attuazione del presente modello di organizzazione, gestione e controllo valgono i principi ed i protocolli di seguito indicati:

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

La conformità alle vigenti norme in materia (leggi, norme tecniche e regolamenti, ecc.) è assicurata attraverso l'adozione di specifiche registrazioni allo scopo di porre sotto controllo:

- l'identificazione e l'accessibilità alle norme in materia applicabili all'organizzazione;
- l'aggiornamento legislativo;
- il controllo periodico della conformità alla normativa applicabile.

(II) Definizione delle risorse, dei ruoli e delle responsabilità per assicurare le attività finalizzate all'attuazione delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori

Per tutte le figure, individuate per la gestione di problematiche inerenti salute e sicurezza nei luoghi di lavoro, sono predefiniti idonei requisiti tecnico-professionali che possono trarre origine anche da specifici disposti normativi; tali requisiti sono in possesso del soggetto preliminarmente all'attribuzione dell'incarico e possono essere conseguiti anche attraverso specifici interventi formativi; essi devono essere mantenuti nel tempo.

L'attribuzione di specifiche responsabilità avviene, 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.

In generale, a titolo esemplificativo, attraverso le modalità definite in procedura:

- sono formalizzate le responsabilità di gestione, coordinamento e controllo all'interno della Società;
- sono correttamente nominati i soggetti previsti dalla normativa in materia di igiene e sicurezza dei luoghi di lavoro (ivi inclusi, nel caso di presenza di cantieri, i soggetti previsti dal titolo IV D.Lgs. 81/2008) e sono loro conferiti correttamente i poteri necessari allo svolgimento del ruolo agli stessi assegnato;
- è definito il sistema di deleghe, dei poteri di firma e di spesa in maniera coerente con le responsabilità assegnate;
- 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;
- si impedisce che vi sia 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 preposti e/o nominati ai sensi della normativa vigente in materia di igiene e sicurezza dei luoghi di lavoro possiedono competenze adeguate ed effettive in materia.

(III) Valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti

L'operazione di individuazione e di rilevazione dei rischi deve essere effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza, sotto la responsabilità 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 (ove previsto), 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 (es. documentazione tecnica, misure strumentali, esiti di sondaggi interni ecc.) devono essere chiari, completi e rappresentare in modo veritiero lo stato dell'arte della Società.

I dati e le informazioni sono raccolti ed elaborati tempestivamente, sotto la supervisione del Datore di Lavoro, anche attraverso soggetti da questo individuati in possesso di idonei requisiti, certificabili nei casi previsti, di competenza tecnica e, se del caso, strumentale. A richiesta, insieme ai dati e alle informazioni, devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni.

Al fine di aggiornare e migliorare costantemente la valutazione dei rischi, gli infortuni sul lavoro e le relative cause devono essere registrati, monitorati ed analizzati dal Servizio di Prevenzione e Protezione.

La redazione del documento di valutazione dei rischi e del piano delle misure di prevenzione e protezione è effettuata sulla base dei criteri definiti preliminarmente, nel rispetto di quanto previsto nell'art.28, d.lgs. 9 aprile 2008, n.81. Detti criteri 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 lavorazioni 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 loro impatto sulle operazioni, processi ed attività;
- eventuali obblighi giuridici applicabili in materia di valutazione dei rischi e di attuazione delle necessarie misure di controllo;
- progettazione di ambienti di lavoro, macchinari ed impianti;
- procedure operative e di lavoro.

(IV) Individuazione e gestione delle misure di protezione collettiva e/o individuale atte a contenere o ad eliminare i rischi

Conseguentemente alla valutazione dei rischi effettuata sia al momento della predisposizione del Documento di Valutazione dei Rischi sia in occasione della predisposizione dei piani operativi della sicurezza, al fine della mitigazione dei rischi, sono individuati i necessari presidi sia individuali sia collettivi atti a tutelare il lavoratore. Attraverso il processo di valutazione dei rischi si disciplina:

- l'identificazione delle attività per le quali prevedere l'impiego di DPI;
- la definizione dei criteri di scelta dei DPI, che devono assicurare l'adeguatezza dei DPI alle tipologie di rischio individuate in fase di valutazione e la loro conformità alle norme tecniche vigenti (ad es. marcatura CE);
- la definizione delle modalità di consegna ed eventualmente di conservazione dei DPI;
- la definizione di un eventuale scadenzario per garantire il mantenimento dei requisiti di protezione.

(V) Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso

La gestione delle emergenze è attuata attraverso specifici piani che prevedono:

- 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;

- pianificazione della verifica dell'efficacia dei piani di gestione delle emergenze;

- aggiornamento delle procedure di emergenza in caso di incidenti o di esiti negativi delle simulazioni periodiche.

Sono definiti specifici piani di gestione delle emergenze. Attraverso detti piani sono individuati i percorsi di esodo e le modalità di attuazione, da parte del personale, delle misure di segnalazione e di gestione delle emergenze.

Tra il personale sono individuati gli addetti agli interventi di emergenza; essi sono in numero sufficiente e preventivamente formati secondo i requisiti di legge.

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

L'efficienza dei piani è garantita attraverso la periodica attività di prova, finalizzate ad assicurare la piena conoscenza da parte del personale delle corrette misure comportamentali e l'adozione di idonei strumenti di registrazioni atti a dare evidenza degli esiti di dette prove e delle attività di verifica e di manutenzione dei presidi predisposti.

(VI) Gestione degli approvvigionamenti e degli acquisti (incluso l'acquisizione della documentazione e delle certificazioni obbligatorie per legge)

Nella definizione, assegnazione ed esecuzione di contratti d'appalto o d'opera o di somministrazione il Datore di Lavoro verifica la sussistenza dei requisiti di cui all'art. 26 del D.Lgs. 81/08.

Il soggetto esecutore delle lavorazioni deve possedere idonei requisiti tecnico-professionali, verificati anche attraverso l'iscrizione alla CCIAA. Esso dovrà dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di Regolarità Contributiva. Se necessario, il soggetto esecutore deve inoltre presentare all'INAIL apposita denuncia per le eventuali variazioni totali o parziali dell'attività già assicurata (in ragione della tipologia di intervento richiesto e sulla base delle informazioni fornite dalla Società).

L'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi deve rilasciare la Dichiarazione di conformità alle regole dell'arte.

Con particolare riferimento a fornitori, installatori e manutentori esterni di macchinari, impianti e di qualsiasi tipo di presidio di sicurezza e attrezzature di lavoro da realizzarsi o installare all'interno di pertinenze poste sotto la responsabilità giuridica del Datore di Lavoro della Società, si prevede l'adozione di specifici protocolli che prevedono:

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

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

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

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

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

- formalizzazione e tracciabilità del controllo da parte dei dirigenti e del Datore di Lavoro del rispetto dei protocolli sin qui elencati.

(VII) Attività di sorveglianza sanitaria

Preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore è necessario verificarne i requisiti sia per quanto riguarda gli aspetti tecnici (cfr. l'attività sensibile successiva: "Competenza, informazione, formazione e consapevolezza dei lavoratori"), sia per quanto riguarda gli aspetti sanitari, in base a quanto evidenziato in fase di valutazione dei rischi, dalla quale, inoltre, scaturisce la formulazione del protocollo sanitario da parte del medico competente.

La verifica dell'idoneità sanitaria del lavoratore è attuata dal Medico Competente della Società che, in ragione delle indicazioni fornite dal datore di lavoro circa la mansione di impiego prevista, sulla base della propria conoscenza dei luoghi di lavoro e delle lavorazioni, e secondo quanto previsto dal protocollo sanitario rilascia il giudizio di idoneità totale o parziale ovvero di inidoneità alla mansione. In ragione della tipologia della lavorazione richiesta e sulla base degli esiti della visita preliminare, il medico competente definisce un protocollo di sorveglianza sanitaria a cui sottopone il lavoratore.

(VIII) Competenza, informazione, formazione e consapevolezza dei lavoratori

Tutto il personale riceve opportune informazioni circa le corrette modalità di espletamento dei propri incarichi, è formato e, nei casi previsti dalla normativa, è addestrato. Di tale formazione e/o addestramento è prevista una verifica documentata. Le attività formative sono erogate attraverso modalità variabili (ad es. formazione frontale, comunicazioni scritte, ecc.) definite sia da scelte della Società sia da quanto previsto dalla normativa vigente.

La scelta del soggetto formatore può essere vincolata da specifici disposti normativi.

In tutti i casi le attività di informazione, formazione e addestramento sono documentate; la documentazione inerente la formazione del personale è registrata ed è impiegata anche al fine dell'attribuzione di nuovi incarichi.

L'attività di formazione è condotta al fine di:

- garantire, anche attraverso un'opportuna pianificazione, che qualsiasi persona sotto il controllo dell'organizzazione sia competente sulla base di un'adeguata istruzione, formazione o esperienza;
- identificare le esigenze di formazione connesse con lo svolgimento delle attività e fornire una formazione o prendere in considerazione altre azioni per soddisfare queste esigenze;
- valutare l'efficacia delle attività di formazione o di altre azioni eventualmente attuate, e mantenere le relative registrazioni;
- garantire che il personale prenda coscienza circa l'impatto effettivo o potenziale del proprio lavoro, i corretti comportamenti da adottare, i propri ruoli e responsabilità.

(IX) Attività di comunicazione, partecipazione e consultazione, gestione delle riunioni periodiche di sicurezza, consultazione dei rappresentanti dei lavoratori per la sicurezza

Le procedure che regolamentano il coinvolgimento e la consultazione del personale definiscono le modalità di:

- comunicazione interna tra i vari livelli e funzioni dell'organizzazione;
- comunicazione con i fornitori ed altri visitatori presenti sul luogo di lavoro;
- ricevimento e risposta alle comunicazioni dalle parti esterne interessate;
- partecipazione dei lavoratori, anche a mezzo delle proprie rappresentanze, attraverso:
  - il loro coinvolgimento nell'identificazione dei pericoli, valutazione dei rischi e definizione delle misure di tutela;

- 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.

(X) Gestione della documentazione e dei sistemi di registrazione al fine di garantire la tracciabilità delle attività

La gestione della documentazione costituisce un requisito essenziale ai fini del mantenimento del Modello di organizzazione, gestione e controllo; attraverso una corretta gestione della documentazione e l'adozione di sistemi di registrazione appropriati si coglie l'obiettivo di dare evidenza di quanto attuato anche assicurando la tracciabilità dei percorsi decisionali.

È altresì rilevante garantire la disponibilità e l'aggiornamento della documentazione sia di origine interna sia di origine esterna (ad es. documentazione relativa a prodotti e sostanze). La gestione della documentazione sia di origine interna sia di origine esterna e la gestione delle registrazioni, che costituiscono documentazione speciale, avviene secondo le procedure del sistema di gestione.

F.5 Ulteriori controlli

In specifica attuazione del disposto dell'art. 18, comma 3-*bis*, D.Lgs. 81/2008, in merito ai doveri di vigilanza del datore di lavoro e dei dirigenti sull'adempimento degli obblighi relativi alla sicurezza sui luoghi di lavoro da parte di preposti, lavoratori, progettisti, fabbricanti e fornitori, installatori e medico competente, sono previsti i seguenti specifici protocolli.

I. Obblighi di vigilanza sui preposti (art. 19, D.Lgs. 81/2008)

Con particolare riferimento alla vigilanza sui preposti, la Società attua specifici protocolli che prevedono che il datore di lavoro, o persona dallo stesso delegata:

- programmi ed effettui controlli a campione in merito all'effettiva istruzione ricevuta dai soggetti che accedono a zone che li espongono ad un rischio grave e specifico;
- programmi ed effettui controlli a campione in merito alle segnalazioni di anomalie da parte dei preposti, nonché alle segnalazioni di anomalie relative a comportamenti dei preposti stessi;
- effettui controlli in merito alle segnalazioni dei preposti relativamente ad anomalie su mezzi ed attrezzature di lavoro e sui mezzi di protezione individuale e su altre situazioni di pericolo, verificando le azioni intraprese dal dirigente per la sicurezza responsabile ed eventuali follow up successivi alle azioni intraprese;
- effettui controlli in merito all'effettiva avvenuta fruizione da parte dei preposti della formazione interna appositamente predisposta.

II. Obblighi di vigilanza sui lavoratori (art. 20, D.Lgs. 81/2008)

Con particolare riferimento alla vigilanza sui lavoratori interni, la Società attua specifici protocolli che prevedono che il datore di lavoro, o persona dallo stesso delegata:

- programmi ed effettui controlli a campione in merito all'effettiva istruzione ricevuta dai lavoratori che accedono a zone che li espongono ad un rischio grave e specifico;
- programmi ed effettui controlli a campione in merito alle segnalazioni di anomalie da parte dei preposti;
- effettui controlli in merito all'effettiva avvenuta fruizione da parte dei lavoratori della formazione interna appositamente predisposta;
- effettui controlli in merito all'effettiva sottoposizione dei lavoratori ai controlli sanitari previsti dalla legge o comunque predisposti dal medico competente.

Con particolare riferimento alla vigilanza sui lavoratori esterni, la Società attua i protocolli previsti per gli obblighi di vigilanza su progettisti, fabbricanti, fornitori, installatori e manutentori esterni.

III. Obblighi di vigilanza sui progettisti (art. 22, D.Lgs. 81/2008)

Con particolare riferimento alle attività di progettazione condotte sia da soggetti interni sia da esterni (cfr. l'attività sensibile "**Manutenzione di attrezzature, macchinari e impianti**"), al fine della realizzazione di macchinari e/o attrezzature da utilizzarsi da parte della Società, la Società stessa attua specifici protocolli, che prevedono che:

- siano rese disponibili, ove possibile, le infrastrutture necessarie per conseguire la conformità normativa di macchinari e/o attrezzature;
- siano definite le modalità di pianificazione, validazione e di controllo della progettazione e dello sviluppo di macchinari e/o attrezzature tenendo conto, oltre che dei requisiti funzionali e prestazionali, anche dei requisiti cogenti applicabili tra cui i requisiti inerenti la sicurezza;
- siano gestite ed identificate le eventuali modifiche occorse nell'ambito della progettazione e dello sviluppo di macchinari e/o attrezzature assoggettando tali attività al processo di validazione e di controllo richiamati al capoverso precedente.

IV. Obblighi di vigilanza su fabbricanti e installatori (art. 23, D.Lgs. 81/2008)

Per le attività di realizzazione e di eventuale installazione di macchinari e/o attrezzature, da utilizzarsi da parte della Società, la Società stessa attua specifici protocolli, che prevedono:

- la definizione delle modalità di realizzazione e di installazione di macchinari e/o attrezzature tenendo conto, oltre che dei requisiti funzionali e prestazionali, anche dei requisiti cogenti applicabili tra cui i requisiti inerenti la sicurezza (ad es. marcatura CE, norme UNI, CEI, ecc.);
- l'impiego di risorse in possesso delle necessarie competenze tecniche e di sicurezza, ove il caso attestate secondo le modalità definite dalla normativa di settore;
- la definizione delle eventuali procedure di messa in esercizio e di omologazione di macchinari e/o attrezzature.

V. Obblighi di vigilanza sul medico competente (art. 25, D.Lgs. 81/2008)

Con particolare riferimento alla vigilanza sul medico competente, la Società attua specifici protocolli che prevedono che il datore di lavoro:

- verifichi il possesso da parte del medico competente dei titoli e dei requisiti previsti dalla legge per lo svolgimento di tale funzione;
- verifichi che il medico competente partecipi regolarmente alle riunioni di coordinamento con il RSPP, i rappresentanti dei lavoratori per la sicurezza e il datore di lavoro stesso, aventi ad oggetto le tematiche della sicurezza sui luoghi di lavoro, incluse quelle relative alle valutazioni dei rischi aziendali e quelle aventi un impatto sulla responsabilità sociale aziendale;
- verifichi la corretta e costante attuazione da parte del medico competente dei protocolli sanitari e delle procedure aziendali relative alla sorveglianza sanitaria.

VI. Ulteriori controlli specifici

Ai sensi del Modello sono istituiti ulteriori controlli specifici volti a fare in modo che il sistema organizzativo della Società, istituito ai sensi delle normative applicabili in materia di sicurezza dei luoghi di lavoro e di prevenzione degli infortuni, sia costantemente monitorato e posto nelle migliori condizioni possibili di funzionamento.

Per il controllo dell'effettiva implementazione delle disposizioni previste dal D.Lgs. 81/2008 e dalla normativa speciale vigente in materia di antinfortunistica, tutela della sicurezza e della salute nei luoghi di lavoro, è previsto che:

- i soggetti qualificati come datore di lavoro, Responsabile del Servizio di prevenzione e protezione e medico competente, aggiornino periodicamente l'OdV della Società in merito alle tematiche relative alla sicurezza sui luoghi di lavoro;

- il Responsabile del Servizio di prevenzione e protezione ed il medico competente comunichino senza indugio le carenze, le anomalie e le inadempienze riscontrate;

- il personale, il rappresentante dei lavoratori per la sicurezza, il medico competente, il Responsabile del Servizio di prevenzione e protezione e il datore di lavoro possano segnalare all'OdV informazioni e notizie sulle eventuali carenze nella tutela della salute e sicurezza nei luoghi di lavoro;

- il datore di lavoro si assicuri che siano nominati tutti i soggetti previsti dalla normativa di settore, che siano muniti di adeguate, chiare e sufficientemente specifiche deleghe, che dispongano delle competenze e qualità necessarie, che abbiano poteri, sufficientemente adeguati all'incarico e che siano effettivamente esercitate le funzioni e le deleghe conferite;

- l'OdV, nell'esercizio delle sue funzioni, possa richiedere l'assistenza dei responsabili della sicurezza nominati dalla Società, nonché di competenti consulenti esterni.

F.6 Attività di audit per la verifica periodica dell'applicazione e dell'efficacia delle procedure

Ai fini delle attività di controllo sopra indicate sono condotte specifiche attività di audit, a cura dell'OdV, anche con la collaborazione dei soggetti aziendali competenti o di consulenti esterni.

L'attività di audit è svolta assicurando che:

- gli audit interni siano condotti ad intervalli pianificati al fine di determinare se il sistema di gestione sia o meno correttamente attuato e mantenuto in tutte le sue parti e sia inoltre efficace per il conseguimento degli obiettivi dell'organizzazione;

- eventuali scostamenti dal sistema siano prontamente gestiti;

- siano trasmesse le informazioni sui risultati degli audit al datore di lavoro.

SEZIONE G

REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO

(art. 25-octies del Decreto)

G.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerati a rischio di commissione in relazione alla Società i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio:

a) **ricettazione,** previsto dall'art. 648 c.p. e costituito dalla condotta di chi, fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare;

b) **riciclaggio,** previsto dall'art. 648-bis c.p. e costituito dalla condotta di chi, fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa;

c) **impiego di denaro, beni o utilità di provenienza illecita,** previsto dall'art. 648-ter c.p. e costituito dalla condotta di chi, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-bis c.p., impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto;

d) **autoriciclaggio,** previsto dall'art. 648-ter.1 c.p. e costituito dalla condotta di chi, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce in attività economiche, finanziarie, imprenditoriali o speculative denaro, beni o altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

G.2 Premessa: il reato di autoriciclaggio

La Legge 15 dicembre 2014, n. 186 ha previsto una serie di disposizioni in materia di emersione e rientro dei capitali detenuti all'estero, nonché il reato di autoriciclaggio con l'inserimento nel codice penale dell'art. 648-ter.1 c.p. Quest'ultima fattispecie si inserisce, quindi, in un sistema di misure volte a contrastare il consolidamento di una precedente situazione di illiceità determinata dalla commissione di un delitto, a cui si associa lo scopo di impedire la circolazione di denaro o di beni di provenienza illecita in un contesto legittimo d'impresa che renderebbe infruttuoso lo svolgimento delle indagini sulla provenienza delittuosa degli stessi[7].

Il tenore letterale della disposizione di cui all'art. 648-ter.1 c.p. indica che la fattispecie di "autoriciclaggio" per perfezionarsi, necessita che ad un reato cosiddetto "presupposto", che generi un profitto anche sotto forma di risparmio segua il reato fine (o presupponente), consistente nel reimpiegare tali proventi in attività d'impresa, con modalità idonee ad ostacolare la provenienza delittuosa dello stesso.

Tuttavia, considerare qualsiasi forma di delitto non colposo come presupposto per l'autoriciclaggio, si tradurrebbe nella non sostenibile pretesa che un ente collettivo debba predisporre un modello di controllo per affrontare qualsivoglia rischio reato. In tal modo verrebbero, pertanto, adottati dei modelli organizzativi su basi di assoluta incertezza e nella totale assenza di oggettivi criteri di riferimento, scomparendo di fatto ogni efficacia in relazione agli auspicati fini di prevenzione. Inoltre, ciò si tradurrebbe in una violazione del principio di legalità e tassatività in materia penale, ribadito anche dall'art. 2 del Decreto, che sancisce come l'ente non può essere ritenuto responsabile per un fatto costituente reato se la sua responsabilità amministrativa in relazione a quel

[7] C. PIERGALLINI, Osservazioni sulla introduzione del reato di autoriciclaggio – Audizione presso la Commissione Giustizia della Camera dei Deputati del 30 luglio 2014 – Proposta di legge c. 2247 in materia di emersione e rientro dei capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale.

reato e le relative sanzioni non sono espressamente previste da una legge entrata in vigore prima della commissione del fatto.

Pertanto, alla luce delle citate garanzie costituzionali richiamate – che l'ordinamento appresta per la responsabilità di natura penalistica – la Società, al fine di gestire il rischio connesso con il reato in oggetto, ha provveduto ad individuare alcune attività sensibili[8] dirette e strumentali[9] per la commissione del reato di autoriciclaggio, ed altresì in via prudenziale, ha ritenuto opportuno, anche in ragione della *ratio legis* dell'art. 648-ter.1 – introdotto all'interno del nostro ordinamento in forza di una legge volta a potenziare la lotta all'evasione fiscale – individuare alcune attività sensibili relative ai processi fiscali e di prevedere per le stesse dei protocolli finalizzati a rafforzare il sistema di controllo interno.

G.3 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita previsti dall'art. 25-octies del Decreto:

- ✓ Gestione delle risorse finanziarie (tramite Home banking);
- ✓ Gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer;
- ✓ Valutazioni e stime di poste soggettive di bilancio; rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti di impresa, anche tramite consulenti esterni;
- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Conferimento e gestione delle consulenze;
- ✓ Gestione del processo di assunzione e gestione del personale (tramite selezione pubblica).

G.4 Protocolli specifici di prevenzione

Per le operazioni riguardanti la **gestione delle risorse finanziarie (tramite Home banking),** la **gestione degli approvvigionamenti (beni, servizi, appalti, software)**, il **conferimento e gestione delle consulenze** e la **gestione del processo di assunzione e gestione del personale (tramite selezione pubblica).** si applica quanto previsto al paragrafo 4 della presente Parte Speciale con riferimento alle corrispondenti attività sensibili.

Inoltre, relativamente alla *gestione delle risorse finanziarie*, i protocolli prevedono che:

- siano effettuate verifiche sulla *tesoreria* (rispetto delle soglie per i pagamenti in contanti, eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità, ecc.);
- siano effettuati controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni tra le società dell'organizzazione;
- i controlli di cui sopra devono tener conto:
  - della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.);

[8] Nel contesto del reato di autoriciclaggio sono considerate "sensibili" quelle attività mediante le quali è possibile commettere in via diretta il reato attraverso l'impiego di risorse di provenienza illecita in attività d'impresa.

[9] Nel contesto del reato di autoriciclaggio sono considerate "strumentali" quelle attività mediante le quali è possibile commettere il delitto presupposto che generi un profitto da "autoriciclare" in attività d'impresa. Si specifica che alcune attività a seconda del tempo, modalità e finalità dell'esecuzione possono risultare al contempo sia sensibili che strumentali.

  - degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese);
  - di eventuali schermi societari e strutture fiduciarie utilizzate per operazioni straordinarie.
- siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio, reimpiego di risorse di provenienza illecita e autoriciclaggio.

Per le operazioni riguardanti la **gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer**, si applica quanto previsto al paragrafo A.5 della presente Parte Speciale, con riferimento alla corrispondente attività sensibile.

Inoltre, i protocolli prevedono che:

- siano identificate, relativamente alla gestione degli adempimenti fiscali, chiare attribuzioni di ruoli e responsabilità;
- sia effettuato un esame storico dei precedenti fiscali (accertamenti tributari, esito dei controlli interni, ecc.);
- sulla base dell'esame storico di cui sopra, siano implementate efficaci procedure interne di rilevazione, misurazione, gestione e controllo dei rischi fiscali;
- gli studi legali e/o i consulenti esterni che supportano la Società nelle attività di gestione degli aspetti fiscali e del contenzioso fiscale siano individuati secondo requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta. Il rapporto con il consulente esterno è formalizzato in un contratto che prevede apposite clausole che richiamino gli adempimenti e le responsabilità derivanti dal Decreto;
- per le fatture ricevute ed emesse dalla Società la registrazione avvenga solo dopo che sia verificata l'effettiva corrispondenza delle stesse – con riferimento sia all'esistenza della transazione, sia all'importo della stessa come indicato in fattura;
- la Società archivia e mantiene la documentazione contabile a supporto delle dichiarazioni fiscali al fine di garantire adeguata tracciabilità.

Per le operazioni riguardanti le **valutazioni e stime di poste soggettive di bilancio; rilevazione, registrazione e rappresentazione dell'attività d'impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti d'impresa, anche tramite consulenti esterni**, si applica quanto previsto al paragrafo E.3 della presente Parte Speciale, con riferimento alla corrispondente attività sensibile.

SEZIONE H

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

(art. 25-*novies* del Decreto)

H.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerate applicabili alla Società le seguenti previsioni incriminatrici:

a) **messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, L. 633/1941 comma 1 lett. a-bis).** Il reato si realizza quando chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma mette a disposizione del pubblico, attraverso un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta o parte di essa. L'interesse giuridico tutelato è il pieno godimento dei diritti di sfruttamento economico dell'opera da parte del titolare.

b) **commissione dei reati previsti dall'art. 171, comma 1, lett. a-bis su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, L. 633/1941 comma 3).** Il reato si realizza quando la fattispecie di cui al punto precedente riguarda una opera altrui non destinata alla pubblicazione ovvero con la deformazione, mutilazione o altra modificazione dell'opera medesima, quando ne risulti offesa all'onore o alla reputazione dell'autore. L'interesse giuridico tutelato è l'onore e la reputazione del titolare del diritto d'autore;

c) **abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis, comma 1, L. 633/1941).** Il reato si realizza quando chiunque, abusivamente, duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE). Anche se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

d) **riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis, comma 2, L. 633/1941).**

Il reato si realizza quando chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE:

- riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca dati in violazione dei diritti del costitutore della banca dati (intendendosi per costitutore di una banca di dati chi effettua investimenti rilevanti per la costituzione di una banca di dati o per la sua verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro);
- ovvero, esegue l'estrazione (intendendosi per estrazione il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma) o il reimpiego (intendendosi per reimpiego qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma) della banca dati in violazione dei diritti dell'istitutore della banca dati;
- ovvero, distribuisce, vende o concede in locazione una banca dati.

e) **abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o**

videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter, L. 633/1941).

Il reato si realizza quando per un uso non personale dell'opera dell'ingegno ed a fini di lucro chiunque:

- a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
- b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
- c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle due lettere precedenti;
- d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, l'apposizione di contrassegno da parte della S.I.A.E., privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato ;
- e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
- f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.
- f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure di protezione tecnologiche ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell' autorità amministrativa o giurisdizionale ;
- h) abusivamente rimuove o altera le informazioni elettroniche di protezione, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche sul regime dei diritti (Le informazioni elettroniche sul regime dei diritti identificano l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti. Tali informazioni possono altresì contenere indicazioni circa i termini o le condizioni d'uso dell'opera o dei materiali, nonché qualunque numero o codice che rappresenti le informazioni stesse o altri elementi di identificazione).

  Affinché la fattispecie si concretizzi devono concorrere sia l'uso non personale che il fine di lucro.

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

Il reato si realizza quando:

- i produttori o gli importatori di supporti informatici, non soggetti al contrassegno SIAE, non comunicano entro il termine di trenta giorni dalla commercializzazione o dall'importazione, alla SIAE stessa i dati necessari alla univoca individuazione dei supporti;
- vengono rese false attestazioni sull'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi (e il delitto di cui si tratta ha natura sussidiaria in quanto ricorre quando il fatto non costituisca un più grave reato).

g) **Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies L. 633/1941).** Il reato si realizza quando a fini fraudolenti si produce, si pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico o privato apparati o parti di apparati atti a decodificare le trasmissioni audiovisive ad accesso limitato. Intendendosi per queste tutti i segnali audiovisivi trasmessi da emittenti italiane od estere in forma tali da essere visibili esclusivamente a gruppi chiusi di utenti selezionati da chi effettua l'emissione del segnale, indipendentemente dall'imposizione di un canone per avere l'accesso. Il delitto di cui si tratta ha natura sussidiaria in quanto ricorre quando il fatto non costituisca un più grave reato.

H.2 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati delitti in materia di violazione del diritto d'autore previsti dall'art. 25-*novies* del Decreto:

- ✓ Gestione dei contenuti e diffusione di materiale tutelato dal diritto d'autore;
- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Gestione e/o manutenzione per conto proprio e/o di terzi di apparecchiature, dispositivi e programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti.

H.3 Protocolli generali di prevenzione

Le procedure di controllo di carattere generale definite al fine di limitare l'insorgere di situazioni di rischio prevedono:

- **Segregazione delle attività**: deve esistere la segregazione delle attività tra chi esegue, chi controlla e chi autorizza;
- **Norme procedurali interne**: devono esistere delle disposizioni aziendali idonee a fornire almeno i principi di riferimento generali per la regolamentazione dell'attività sensibile;
- **Conferimento formale delle deleghe con poteri di firma**: devono esistere regole formalizzate per l'esercizio dei poteri di firma e dei poteri autorizzativi interni;
- **Tracciabilità:** i soggetti, le funzioni interessate e/o i sistemi informativi utilizzati devono assicurare l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni della società e le modalità di gestione delle risorse finanziarie.

H.4 Protocolli specifici di prevenzione

Installazione di software

Procedura: è prevista la formalizzazione di una procedura per la gestione del processo di installazione del software che prevede:

- la definizione di ruoli e responsabilità nell'ambito dell'attività ed una limitazione delle abilitazioni all'esecuzione di installazioni di nuovo software alle persone che ne hanno effettivamente la responsabilità;
- la gestione del processo di installazione integrato con un processo di monitoraggio delle licenze disponibili rispetto a quelle installate;
- il monitoraggio in merito al corretto utilizzo di software protetti da licenze;
- il divieto espresso per i dipendenti di installare software non autorizzato.

Qualora le installazioni siano fatte per conto di terzi sono definite, tra le parti le responsabilità e le modalità di gestione delle licenze.
Audit: periodicamente, attraverso la rete aziendale viene effettuata una attività di verifica del software installato su tutte le macchine che consente di identificare eventuali installazioni non autorizzate.

Acquisto di un prodotto o di servizi di sviluppo software
Procedura: è prevista la formalizzazione di una procedura per la gestione del processo di approvvigionamento di prodotti o servizi che prevede:

- la determinazione dei requisiti minimi in possesso dei soggetti offerenti e la fissazione dei criteri di valutazione delle offerte prima della ricezione delle stesse;
- l'identificazione di una funzione/unità responsabile della definizione delle specifiche tecniche e della valutazione delle offerte;
- la nomina di un responsabile dell'esecuzione del contratto ("gestore del contratto") con indicazione di compiti, poteri e responsabilità a esso attribuiti;
- l'autorizzazione da parte di posizione superiore abilitata che sia diversa dal gestore del contratto in caso di modifiche/integrazioni e/o rinnovi dello stesso.

Valutazione del prodotto: in fase di qualifica del fornitore, la funzione responsabile della definizione delle specifiche tecniche verifica le caratteristiche del prodotto e la documentazione a supporto di marchi, brevetti, diritti d'autore o di altre proprietà intellettuali. In fase di fornitura, la funzione responsabile verifica la qualità e le caratteristiche dei prodotti e la loro rispondenza alle specifiche definite nei contratti.
Clausole contrattuali: è previsto l'inserimento di specifiche clausole contrattuali che disciplinano la responsabilità del fornitore relativamente a marchi, brevetti, diritti d'autore ed altre proprietà intellettuali.
Scelta della controparte: è vietato intrattenere rapporti, negoziare o stipulare o porre in esecuzione contratti o atti con soggetti indicati nelle liste nominative, stilate da organismi ufficiali (es. liste approvate dall'Unione europea per l'applicazione delle misure di congelamento e di divieto di prestazione dei servizi finanziari, diffuse dall'UIF), che permettano di effettuare gli opportuni controlli prima di procedere alla stipulazione di un contratto (c.d. Liste di Riferimento).

Gestione dei contenuti e delle attività di pubblicazione
Procedura: è prevista la formalizzazione di una procedura che disciplina la diffusione di materiale tutelato dal diritto d'autore e che prevede:

- la definizione di ruoli e responsabilità nell'ambito dell'attività;
- l'espresso divieto di utilizzo e diffusione, senza l'acquisto dei relativi diritti, di materiale tutelato;
- le modalità di acquisizione del materiale tutelato;
- le modalità di diffusione del materiale tutelato.

Nel caso di erogazione a terzi di servizi di gestione di strumenti di memorizzazione e/o diffusione delle informazioni (ad es. repositories, siti Internet, etc.) sono chiarite con la controparte le responsabilità in merito alla gestione dei contenuti ed il divieto di gestione di contenuti in violazione della normativa, incluso quanto previsto in merito ai diritti di autore.

H.5 Attività sensibili affidate, in tutto o in parte, a soggetti terzi

Nel caso in cui una delle sopra citate attività sensibili sia affidata, in tutto o in parte, a soggetti terzi in virtù di appositi contratti di servizio occorre che in essi sia prevista, fra le altre:

- la sottoscrizione di una dichiarazione con cui i terzi attestino di conoscere e si obblighino a rispettare, nell'espletamento delle attività per conto di IT CIty, i principi contenuti nel Codice Etico e gli standard di controllo specifici del Modello;
- la comunicazione (in caso di società di diritto italiano) circa l'avvenuta adozione o meno, da parte dello stesso fornitore, di un modello di organizzazione, gestione e controllo ex d.lgs. n. 231/2001;
- l'obbligo da parte della società che presta il servizio di garantire la veridicità e completezza della documentazione o delle informazioni comunicate alla società beneficiaria;
- il potere dell'Organismo di Vigilanza della società beneficiaria del servizio di richiedere informazioni alla società che presta il servizio al fine di verificare il suo corretto svolgimento;
- la facoltà di risolvere i contratti in questione in caso di violazione di tali obblighi.

SEZIONE I

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

(art. 25-*decies* del Decreto)

I.1 Fattispecie incriminatrice applicabile

Sulla base delle analisi condotte è considerata potenzialmente applicabile alla Società la fattispecie incriminatrice dell'**induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria**.

I.2 Attività sensibili e prevenzione

La Società ha individuato le seguenti attività sensibili nell'ambito delle quali, potenzialmente, potrebbe essere perpetrato il fatto di reato di cui all'art. 377-*bis* c.p.:

- ✓ Gestione dei rapporti con l'Autorità Giudiziaria, anche tramite consulenti esterni.

Si ritiene che, date le molteplici attività attraverso cui potrebbe essere integrata tale fattispecie nei rapporti con l'Autorità giudiziaria (a titolo esemplificativo, in occasione di procedimenti penali in cui un dipendente sia chiamato a rendere testimonianza), i principi contenuti nel Codice Etico nonché quanto previsto al Paragrafo A5 della Sezione A della presente Parte Speciale, costituiscano lo strumento più adeguato per prevenire la commissione di tale reato.

Tutti i destinatari del Modello, quindi, al fine di evitare condotte che possano integrare tale delitto, adottano prassi e comportamenti che siano rispettosi del Codice Etico e di quanto previsto dal richiamato Paragrafo A5 della Sezione A della presente Parte Speciale; in particolare, i destinatari del Modello seguono i principi etici della Società relativi ai rapporti con l'Autorità giudiziaria.

SEZIONE J

REATI AMBIENTALI

(art. 25-*undecies* del Decreto)

J.1 Fattispecie incriminatrici applicabili

Sulla base delle analisi condotte sono considerati applicabili alla Società i seguenti reati ambientali:

a) **reati connessi alla gestione dei rifiuti,** previsti dall'art. 256, commi 1, 3, 5 e 6, D.Lgs. 152/2006; tali ipotesi di reato si configurano nel caso in cui sia svolta l'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti – sia pericolosi che non pericolosi – in mancanza della prescritta autorizzazione; sia effettuato illegittimamente il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi; sia realizzata o gestita una discarica non autorizzata, anche eventualmente destinata ai rifiuti pericolosi; siano svolte attività non consentite di miscelazione di rifiuti;

b) **predisposizione o utilizzo di un certificato di analisi rifiuti falso,** previsto dall'art. 258, comma 4, D.Lgs. 152/2006 e che punisce chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, nonché chi fa uso di un certificato falso durante il trasporto;

c) **traffico illecito di rifiuti,** previsto dall'art. 259, comma 1, D.Lgs. 152/2006 e che punisce chiunque effettui una spedizione di rifiuti costituente traffico illecito ai sensi dell'art. 2 del regolamento (CEE) 1° febbraio 1993, n. 259, ovvero effettui una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'art. 1, comma 3, lettere a), b), c) e d) dello stesso;

d) **attività organizzate per il traffico illecito di rifiuti,** previsto dall'art. 260, commi 1 e 2, D.Lgs. 152/2006 e che punisce chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa o comunque gestisce abusivamente ingenti quantitativi di rifiuti;

e) **falsificazione di un certificato di analisi di rifiuti utilizzato nell'ambito del sistema di controllo della tracciabilità degli stessi, utilizzo di un certificato o di una copia cartacea della scheda SISTRI fraudolentemente alterati,** previsto dall'art. 260-*bis*, commi 6, 7, secondo e terzo periodo, e 8, D.Lgs. 152/2006; tali ipotesi di reato puniscono chiunque, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, fornisca false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, inserisca un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti, nonché durante il trasporto faccia uso di un certificato di analisi di rifuti contente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati. Il reato punisce inoltre il trasportatore che accompagni il trasporto dei rifiuti con una copia cartacea della scheda SISTRI-Area Movimentazione fraudolentemente alterata;

J.2 Attività sensibili

La Società ha individuato la seguente attività sensibile, nell'ambito della quale, potenzialmente, potrebbero essere commessi i citati reati ambientali previsti dall'art. 25-*undecies* del Decreto:

✓ Gestione delle attività di smaltimento dei rifiuti.

J.3 Protocolli generali di prevenzione

a) Attribuzione di ruoli responsabilità in ambito ambientale

La Società adotti, con riferimento ai soggetti responsabili di attività aventi potenziali impatti sull'ambiente, un sistema di formale attribuzione delle responsabilità tramite deleghe e procure formalmente accettate

b) Gestione delle risorse umane: competenza, formazione e consapevolezza

La Società adotti una procedura che regolamenti il processo di informazione, formazione e organizzazione dei corsi di addestramento, anche in materia ambientale, definendo in particolare:

- ruoli e responsabilità inerenti la formazione sugli aspetti ambientali e sulle relative procedure, alla quale tutti i Dipendenti della Società devono obbligatoriamente sottoporsi;
- criteri di aggiornamento e/o integrazione della formazione, in considerazione di eventuali trasferimenti o cambi di mansioni, introduzione di nuove attrezzature o tecnologie che possano determinare impatti ambientali significativi, ecc..

c) Gestione della documentazione

La Società adotti un sistema formalizzato che disciplini le attività di controllo della documentazione inerente la Gestione Ambientale definendo modalità di registrazione, gestione, archiviazione e conservazione della documentazione prodotta (ad es. modalità di archiviazione e di protocollazione dei documenti, a garanzia di adeguata tracciabilità e verificabilità).

J.4 Protocolli specifici di prevenzione

Per le operazioni riguardanti la **gestione delle attività di smaltimento dei rifiuti,** i protocolli prevedono che siano definiti:

- nell'ambito della **produzione dei rifiuti**:
  - al momento della definizione dei requisiti dei prodotti da acquistare sia tenuto in debito conto la gestione del "fine vita" del prodotto stesso, indirizzando le scelte verso quei prodotti che possono essere in toto o in parte destinati al recupero;
  - sia favorita la riduzione dei rifiuti da inviare a discarica favorendo il riuso degli stessi.
- nell'ambito delle attività di **raccolta dei rifiuti**, sia adottato uno strumento organizzativo che:
  - disciplini ruoli e responsabilità per assicurare l'accertamento della corretta codifica dei rifiuti anche attraverso l'individuazione di idonei soggetti atti all'eventuale controllo analitico degli stessi;
  - assicuri la corretta differenziazione dei rifiuti e prevenga ogni miscelazione illecita;
  - assicuri la corretta gestione dei depositi temporanei dei rifiuti sulla base della tipologia e dei quantitativi di rifiuti prodotti;
  - valuti l'eventuale necessità di autorizzazioni per lo svolgimento delle attività di raccolta (ad es. stoccaggi) e attivi le necessarie procedure per l'ottenimento delle stesse;
  - pianifichi e assicuri il monitoraggio dell'attività comunicandone le risultanze ai soggetti preposti;
  - assicuri la disponibilità della documentazione pertinente (ad es. registrazioni relative ai controlli analitici);
- nell'ambito delle attività di **trasporto dei rifiuti**, sia adottato uno strumento organizzativo che:
  - disciplini ruoli e responsabilità per assicurare che il soggetto individuato per l'esecuzione dei trasporti possegga i prescritti requisiti richiesti dalla normativa vigente;
  - assicuri, nel caso di trasporto condotto in proprio, il possesso dei prescritti requisiti richiesti dalla normativa vigente;
  - assicuri la corretta gestione degli adempimenti per controllare il trasporto dei rifiuti fino al momento dell'arrivo alla destinazione finale (gestione dei formulari e dei registri carico/ scarico, gestione SISTRI);

  - assicuri la disponibilità della documentazione pertinente (ad es. registri, formulari, documentazione analitica di accompagnamento ecc.);

- nell'ambito delle attività di **smaltimento dei rifiuti** sia adottato uno strumento organizzativo che:
  - disciplini ruoli e responsabilità per assicurare che il soggetto individuato per lo smaltimento possegga i prescritti requisiti previsti dalla normativa vigente;
  - assicuri la corretta gestione degli adempimenti per controllare che lo smaltimento sia condotto secondo liceità;
  - assicuri la disponibilità della documentazione pertinente.

SEZIONE K

IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

(art. 25-*duodecies* del Decreto)

K.1 Fattispecie incriminatrice applicabile

Sulla base delle analisi condotte è considerato applicabile alla Società l'art. 22, comma 12-*bis*, del Decreto Legislativo 25 luglio 1998, n. 286, relativo al reato di **impiego di cittadini di paesi terzi il cui soggiorno è irregolare**, costituito dalla condotta di chi, in qualità di datore di lavoro, occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, ovvero sia revocato o annullato se i lavoratori occupati sono (alternativamente):

- in numero superiore a tre;
- minori in età non lavorativa;

sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'art. 603-bis c.p., cioè esposti a situazioni di grave pericolo, con riferimento alle prestazioni da svolgere e alle condizioni di lavoro.

K.2 Attività sensibili

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbe essere commesso il reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare previsto dall'art. 25-*duodecies* del Decreto:

- ✓ Gestione degli approvvigionamenti (beni, servizi, appalti, software);
- ✓ Gestione del processo di assunzione e gestione del personale (tramite selezione pubblica).

K.3 Protocolli specifici di prevenzione

Per le operazioni riguardanti la **gestione degli approvvigionamenti (beni, servizi, appalti, software),** si applica quanto previsto al paragrafo 4 della presente Parte Speciale, con riferimento alla corrispondente attività sensibile.

Inoltre, i protocolli prevedono che:

- sia verificata la sussistenza dei requisiti normativi di regolarità della controparte tramite la consegna della documentazione prevista dalla legge;
- siano effettuate verifiche sul personale impiegato dalla controparte.

Per le operazioni riguardanti la **gestione del processo di assunzione e gestione del personale (tramite selezione pubblica)**, si applica quanto previsto al paragrafo 4 della presente Parte Speciale, con riferimento alla corrispondente attività sensibile.

Inoltre, i protocolli prevedono che:

- in fase di assunzione, sia verificata nel rispetto della normativa vigente, copia del regolare permesso di soggiorno, del quale verifichi la scadenza al fine di monitorarne la validità durante il prosieguo del rapporto di lavoro;
- la documentazione sia conservata, ad opera della funzione competente, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- la validità dei permessi di soggiorno sia monitorata.

SEZIONE L

REATI TRIBUTARI

(art. 25-*quinquiesdecies* del Decreto)

L.1. Fattispecie incriminatrice applicabile

Con riferimento all'attività svolta dalla Società IT.CITY S.p.A. ed ai rischi in cui potrebbe incorrere, di seguito sono stati indicati i reati ritenuti potenzialmente inerenti per la Società.

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, d.lgs. 74/2000;
- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, d.lgs. 74/2000;
- dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, d.lgs. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, d.lgs. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, d.lgs. 74/2000;
- occultamento o distruzione di documenti contabili, previsto dall'articolo 10, d.lgs. 74/2000;
- sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, d.lgs. 74/2000.

L.2. Attività sensibili

Le aree sensibili sono stabilite tenendo conto della natura e delle caratteristiche della Società con riferimento alle attività, ai processi decisionali, ai controlli interni e ai rapporti con soggetti nell'ambito dei quali può essere consumato il reato.

I processi interessati riguardano le seguenti aree:

- Area economico – finanziaria, con riferimento alla gestione della fiscalità (anche mediante la registrazione di fatture attive e passive), anche tramite outsourcer, e alle valutazioni e stime di poste soggettive di bilancio; alla rilevazione, registrazione e rappresentazione dell'attività d'impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti d'impresa, anche tramite consulenti esterni.

L.3. Protocolli specifici di prevenzione

Al fine di limitare l'insorgere di situazioni di rischio, nello svolgimento delle proprie attività i responsabili dei vari processi potenzialmente impattati dai reati tributari dovranno attenersi, oltre agli standard di controllo indicati nei punti seguenti, a quanto definito nei "Regolamenti", nei "Manuali di processo", nelle "Disposizioni operative", nel "Codice Etico" e nelle procedure relative alle aree di attività a rischio.

Processo di gestione della fiscalità

Gli standard di controllo relativi all'area economico finanziaria con riferimento alla gestione del processo di pagamento e incassi sono definiti, anche per quanto riguarda la prevenzione dei reati tributari, negli *Standard di controllo specifici* della Sezione G del Modello.

Allegato 1: Dichiarazione di responsabilità e di assenza di conflitti di interesse

Il sottoscritto dichiara di conoscere il contenuto del D. Lgs. 231/01, della legge 190/2012, del D. Lgs. 33/2013 e del Modello di organizzazione, gestione e controllo adottato da IT City, volto a prevenire i reati previsti dalla normativa citata.
Il sottoscritto dichiara di non aver posto in essere azioni non in linea con il citato Modello. Più in particolare dichiara che:

- non ha posto in essere azioni non in linea con il Codice etico aziendale;
- non si è mai trovato in situazioni tali da configurare un conflitto di interessi nell'ambito di rapporti intrattenuti con rappresentanti di Pubbliche Amministrazioni, italiane o estere;
- ha sempre rispettato i poteri di delega ed i limiti di firma stabiliti;
- ha rispettato gli obblighi di informativa all'Organismo di vigilanza, riportati nel "Modello 231";
- ha sempre rispettato le procedure emesse dalla Società e le altre misure previste dal Modello.

Il sottoscritto conferma inoltre di non essere venuto a conoscenza (anche in virtù delle attività di controllo effettuate) di elementi tali da dover essere comunicati all'Organismo di vigilanza in quanto capaci di influire sull'adeguatezza, completezza ed efficacia del Modello e circa la sua effettiva applicazione.
Il sottoscritto si impegna a segnalare tempestivamente all'Organismo di Vigilanza qualsiasi variazione in relazione ai propri conflitti di interesse rispetto quanto affermato nella presente dichiarazione.

In fede

Nome e cognome .....

Posizione .....

Data .....

Allegato 2: Dichiarazione e clausola risolutiva da inserire negli incarichi a collaboratori e consulenti esterni

Il sottoscritto dichiara di essere a conoscenza delle disposizioni di cui al Decreto Legislativo 8 giugno 200l n. 231, e successive integrazioni, nonché delle norme del Codice Etico e di quelle previste dal Modello 231 della Società in relazione al presente incarico.
Il sottoscritto si impegna, pertanto, a tenere un comportamento in linea con il suddetto Codice Etico e con il Modello, per le parti applicabili, e comunque tale da non esporre la Società al rischio dell'applicazione delle sanzioni previste dal suddetto Decreto Legislativo.

L'inosservanza di tale impegno da parte del sottoscritto costituirà grave inadempimento contrattuale e legittimerà la Società a risolvere il presente contratto con effetto immediato, ai sensi e per gli effetti di cui all' art. 1456 Cod. Civ., fermo restando il risarcimento dei danni.

N.B. Da inserire nei contratti con prestatori di servizi professionali, consulenti e collaboratori coordinati e continuativi.

Allegato 3: Dichiarazione e clausola risolutiva da inserire negli incarichi a fornitori

Il Fornitore dichiara di essere a conoscenza delle disposizioni di cui al Decreto Legislativo 8 giugno 200l n. 231, e successive integrazioni, nonché delle norme del Codice Etico e di quelle previste dal Modello 231 di IT.CITY SpA in relazione al presente incarico.
Il Fornitore e i suoi dipendenti si impegnano, pertanto, a tenere un comportamento in linea con il suddetto Codice Etico e con il Modello, per le parti applicabili, e comunque tale da non esporre la IT.CITY SpA al rischio dell'applicazione delle sanzioni previste dal suddetto Decreto Legislativo.

L'inosservanza di tale impegno da parte del Fornitore costituirà grave inadempimento contrattuale e legittimerà IT.CITY SpA a risolvere il presente contratto con effetto immediato, ai sensi e per gli effetti di cui all' art. 1456 Cod. Civ., fermo restando il risarcimento dei danni.