

D. LGS. 231/2001
RESPONSABILITÀ AMMINISTRATIVA
DELLE PERSONE GIURIDICHE

IL MODELLO DI ORGANIZZAZIONE
GESTIONE E CONTROLLO

APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE NELLA SEDUTA
DEL 9 MARZO 2018

SOMMARIO

Parte Generale.....5

1. Il Decreto legislativo n. 231/2001.....5

 1.1 Premessa.....5

 1.2 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni anche prive di personalità giuridica.....6

 1.3 L’adozione del “Modello” quale possibile esimente della responsabilità amministrativa.....9

2. Adozione del Modello in TIP – Tamburi Investment Partners S.p.A. 10

 2.1. Obiettivi perseguiti con l’adozione del Modello 10

 2.2 Adozione del Modello e costituzione dell’Organismo di Vigilanza 11

 2.3. La costruzione del Modello e la sua struttura 11

3. L’Organismo di Vigilanza 13

 3.1 Composizione dell’Organismo di Vigilanza..... 13

 3.2. Durata in carica e sostituzione dei componenti 13

 3.3. Cause di ineleggibilità ed incompatibilità..... 14

 3.4 Funzioni e poteri dell’Organismo di Vigilanza..... 14

 3.5 Reporting verso il Consiglio di Amministrazione..... 15

4. Flussi informativi e segnalazioni verso l’Organismo di Vigilanza 16

 4.1 Flussi informativi nei confronti dell’Organismo di Vigilanza 16

 4.2 Segnalazioni all’Organismo di Vigilanza..... 16

5. Sistema Disciplinare..... 17

 5.1 Funzioni del sistema disciplinare 17

 5.2 Misure nei confronti di quadri ed impiegati..... 18

 5.3 Misure nei confronti degli amministratori..... 19

 5.4. Misure nei confronti dei sindaci..... 19

 5.5 Misure nei confronti di consulenti e Partner 19

6. Regole di comportamento e Codice Etico..... 19

7. Diffusione e informazione sul Modello..... 19

8. Formazione sul Modello 20

Parte Speciale 22

9. Finalità..... 22

10. La Società: attività e Governance 23

11. Classificazione dei reati presupposto in relazione alle aree e operazioni a rischio 25

 11.1 I reati nei confronti della pubblica amministrazione – artt. 24 e 25 D.Lgs. n. 231/01..... 25

 11.1.1 Le attività sensibili ai fini del D.Lgs. n. 231/01..... 27

 11.2 I delitti informatici e trattamento illecito dei dati – art. 24*bis*, D.Lgs. 231/01 28

 11.2.1 Le attività sensibili ai fini del D.Lgs. 231/01 29

 11.2.2 I presupposti ai protocolli di prevenzione..... 30

11.2.2.1 Pianificazione.....	30
11.2.2.2 Il Modello Organizzativo Privacy	30
11.2.2.3 Predisposizione e organizzazione dell'organigramma della sicurezza informatica e le relative formalizzazioni di incarichi interni ed esterni	31
11.2.2.4 Applicazione di protocolli e procedure specifiche	31
11.2.2.5 La programmazione dei programmi di informazione e formazione	32
11.2.2.6 Il Controllo e le azioni correttive	32
11.2.2.7 I piani di miglioramento	33
11.3 I delitti di criminalità organizzata – art. 24 ^{ter} , D.Lgs. n. 231/01	33
11.3.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	34
11.4 I reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento – art. 25 ^{bis} , D.Lgs. n. 231/01	35
11.5 I delitti contro l'industria e il commercio – art. 25 ^{bis} .1, D.Lgs. n. 231/01	35
11.6 I reati societari – art. 25 ^{ter} , D.Lgs. n. 231/01	35
11.6.1 Le attività sensibili ai fini del D.Lgs. 231/01	39
11.7 I delitti con finalità di terrorismo o di eversione dell'ordine democratico – art. 25 ^{quater} , D.Lgs. n. 231/01	40
11.7.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	40
11.8 I delitti contro la persona – artt. 25 ^{quater} .1 – 25 ^{quinquies} , D.Lgs. n. 231/01	41
11.8.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	42
11.9 Gli abusi di mercato – art. 25 ^{sexies} , D.Lgs. n. 231/01	43
11.9.1 Le attività sensibili ai fini del D.Lgs. 231/01	44
11.10 I reati in ambito di igiene e sicurezza sul lavoro – art. 25 ^{septies} , D.Lgs. n. 231/01	44
11.10.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	45
11.11 I reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché auto riciclaggio – art. 25 ^{octies} , d.Lgs. n. 231/01	46
11.11.1 Le attività sensibili ai fini del D.Lgs. 231/01	46
11.12 I delitti in materia di violazione del diritto d'autore – art. 25 ^{novies} , D.Lgs. n. 231/01	47
11.12.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	49
11.13 I delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria – art. 25 ^{decies} , D.Lgs. n. 231/01	49
11.13.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	50
11.14 I reati ambientali – art. 25 ^{undecies} , D.Lgs. n. 231/01	50
11.14.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	51
11.15 I reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare – art. 25 ^{duodecies} , D.Lgs. n. 231/01	51
11.15.1 Le attività sensibili ai fini del D.Lgs. n. 231/01	52
12. Protocolli operativi	53

12.1 Gestione dei contenziosi giudiziari e stragiudiziali (es. accordi transattivi, contenzioso giuslavoristico, contenzioso tributario).....	53
12.2 Rapporti con l’Autorità Giudiziaria nell’ambito di procedimenti penali.....	55
12.3 Gestione dei rapporti con l’Amministrazione Finanziaria (es. predisposizione della dichiarazione dei redditi o dei sostituti di imposta).....	56
12.4 Gestione degli adempimenti e delle comunicazioni con le Autorità pubbliche di vigilanza.....	58
12.5 Gestione dei rapporti, anche in caso di ispezioni, con soggetti pubblicisticamente qualificati, con Autorità di Vigilanza e controllo in materia fiscale, tributaria, societaria e finanziaria, ambientale, previdenziale, sanitaria, di sicurezza e igiene sul lavoro, prevenzione degli infortuni sul lavoro e assistenziale in genere, di immigrazione, espatrio da parte di personale proveniente da paesi extracomunitari	60
12.6 Richiesta, ottenimento e gestione dei rapporti con soggetti pubblicisticamente qualificati in occasione del conseguimento o rinnovo di abilitazioni, concessioni, autorizzazioni, certificazioni e licenze, comunque denominate, rilasciate per l’esercizio dell’attività d’impresa.....	62
12.7 Gestione dei flussi finanziari	63
12.8 Predisposizione di bilanci, relazioni e comunicazioni sociali in genere.....	65
12.9 Gestione della clientela.....	68
12.10 Selezione e gestione dei fornitori.....	72
12.11 Selezione e gestione dei consulenti	74
12.12 Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale	76
12.13 Gestione delle c.d. informazioni privilegiate e manipolazione del mercato	79
12.14 Gestione dei doni e regalie ricevuti dai dipendenti.....	82
12.15 Utilizzo di opere di ingegno coperte dal diritto d’autore.....	83
12.16 Utilizzo dei sistemi informatici da parte degli utenti.....	84
12.17 Utilizzo e gestione dei sistemi informatici da parte dell’Amministratore di Sistema e di utilizzatori di pc Administrator oppure utenti con accessi/permessi privilegiati.....	86
12.18 Utilizzo di firma digitale.....	89
12.19 Utilizzo della posta certificata	90
12.20 Smarrimento di strumenti informatici	91
12.21 Gestione delle licenze relative ai programmi, applicativi e software in uso.....	92
12.22 Gestione dei rapporti con il Collegio Sindacale e con la Società di revisione	93
12.23 Gestione delle situazioni di conflitto di interesse degli Amministratori	94
12.24 Gestione dei prodotti e rifiuti, compilazione dei registri di controllo e flussi informativi verso le Autorità di Vigilanza.....	96
12.25 Le attività d’ufficio	97
12.26 I rapporti con i soggetti esterni ai sensi dell’art. 26 del D.Lgs. n. 81/2008 (in particolare, affidamento dei lavori all’impresa appaltatrice o a lavoratori autonomi all’interno dell’Ente).....	98

Parte Generale

1. Il Decreto legislativo n. 231/2001

1.1 Premessa

Il D.Lgs. n. 231/2001 (di seguito anche il “Decreto”) sulla responsabilità amministrativa degli enti per illeciti dipendenti da reato è stato emanato in esecuzione di una serie di convenzioni internazionali ed è entrato in vigore il 4 luglio 2001.

Inizialmente circoscritto a fattispecie di reato a danno delle Pubbliche Amministrazioni, il Decreto è stato successivamente esteso ad altre tipologie di illecito, quali “delitti informatici”, “delitti di criminalità organizzata”, “reati in materia societaria”, “delitti aventi finalità di terrorismo”, “reati di abuso di informazioni privilegiate e di manipolazione del mercato”, “reati colposi in materia di salute e sicurezza sul lavoro”, “reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita”, “delitti in materia di violazione del diritto d’autore”, “reati ambientali” e “reati transnazionali”.

Recentemente, il Decreto ha recepito anche ulteriori fattispecie di illecito, quali il “reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare”, la “corruzione tra privati” (quest’ultima accolta nell’ambito del già esistente articolo 25^{ter} del Decreto - reati in materia societaria) e il reato di “autoriciclaggio” (quest’ultima accolta nell’ambito del già esistente articolo 25^{octies} del Decreto – reati di ricettazione, riciclaggio ed impiego di denaro, beni ed utilità di provenienza illecita).

In sintesi la normativa prevede che ciascun ente, al fine di escludere proprie responsabilità amministrative in caso di reati compiuti da soggetti “apicali” o dipendenti/collaboratori della stessa, possa:

- adottare ed efficacemente attuare modelli di organizzazione, gestione e controllo (di seguito anche il “Modello”) idonei a prevenire le fattispecie di illecito sopra elencate;
- vigilare sul funzionamento ed osservanza del Modello e curarne l’aggiornamento attraverso apposito Organismo di Vigilanza (di seguito anche “OdV”).

Fra le esimenti di responsabilità definite dalla normativa è prevista anche la verifica periodica e l’aggiornamento del Modello a fronte di:

- mutamenti che hanno riguardato l’assetto organizzativo dell’ente;
- mutamenti che hanno riguardato l’attività svolta dall’ente e/o i prodotti offerti dallo stesso alla propria clientela;
- accertamento di eventuali violazioni delle regole organizzative previste dal Modello.

Tale aggiornamento si rende peraltro necessario anche in relazione all’evoluzione legislativa (estensione dei reati) ed alla giurisprudenza in materia (es. sentenze, ordinanze, ecc.).

1.2 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni anche prive di personalità giuridica

Il Decreto 231/2001 dal titolo “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” detta norme in ordine alla “responsabilità degli enti per gli illeciti amministrativi dipendenti da reato”.

Il legislatore ha inteso adeguare la normativa italiana in materia di responsabilità delle persone giuridiche alle 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 di Bruxelles del 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.

I reati presupposto a cui il Decreto si riferisce sono quelli previsti dalla Sez. III del Capo I del D.lgs. 231/2001 (artt. 24 e ss.), che possono essere ricomprese, per comodità espositiva, nelle seguenti categorie:

- **reati commessi nei rapporti con la Pubblica Amministrazione** (articoli 24 e 25 del d.lgs. 231/2001);
- **delitti informatici e trattamento illecito dei dati**, introdotti dall'articolo 7 della Legge 18 marzo 2008, n. 48, che ha inserito nel d.lgs. 231/2001 l'articolo 24 *bis*;
- **delitti di criminalità organizzata**, introdotti dall'articolo 2, comma 29, della Legge 15 luglio 2009, n. 94, che ha inserito nel d.lgs. 231/2001 l'articolo 24-ter;
- **reati in tema di falsità in monete, carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento**, introdotti dall'articolo 6 della Legge 23 novembre 2001, n. 406, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *bis*, come modificato dall'articolo 15, comma 7, lett. a), della Legge 23 luglio 2009, n. 99;
- **delitti contro l'industria e il commercio**, introdotti dall'articolo 15, comma 7, lett. b), della Legge 23 luglio 2009, n. 99, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *bis* 1;
- **reati in materia societaria**, introdotti dal Decreto Legislativo 11 aprile 2002, n. 61, che ha inserito nel d.lgs. 231/2001 l'articolo 25-ter. Tale articolo è stato successivamente modificato dalla Legge 6 novembre 2012, n. 190 che ha introdotto l'articolo 2635 c.c.;
- **delitti aventi finalità di terrorismo o di eversione dell'ordine democratico**, introdotti dalla Legge 14 gennaio 2003, n. 7, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *quater*;
- **delitti di pratiche di mutilazione degli organi genitali femminili**, introdotti dalla Legge 9 gennaio 2006, n. 7, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *quater*.1;
- **delitti contro la personalità individuale**, introdotti dalla Legge 11 agosto 2003, n. 228, che ha inserito nel d.lgs. 231/2001 l'articolo 25-*quinquies*, come modificato dall'articolo 10 della Legge 6 febbraio 2006, n. 38;
- **reati di abuso di informazioni privilegiate e di manipolazione del mercato**, previsti dalla Legge 18 aprile 2005, n. 62, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *sexies*;
- **reati di omicidio colposo e lesioni colpose gravi o gravissime**, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e sicurezza dei lavoratori, introdotti dalla Legge 3 agosto 2007, n. 123, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *septies*, come

- modificato dall'articolo 300 del Decreto Legislativo 9 aprile 2008, n. 81;
- **reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio**¹, introdotti dal Decreto Legislativo 21 novembre 2007, n. 231, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *octies*;
 - **delitti in materia di violazione del diritto d'autore**, introdotti dall'articolo 15, comma 7, lett. c), della Legge 23 luglio 2009, n. 99, che ha inserito nel d.lgs. 231/2001 l'articolo 25 *novies*;
 - **reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**, introdotto dall'art. 4 della Legge 3 agosto 2009, n. 116, come sostituito dall'art. 2, co. 1, Decreto Legislativo 7 luglio 2011, n. 121, che ha inserito nel d.lgs. n. 231/2001 l'articolo 25-*decies*;
 - **reati ambientali**, introdotti dall'art. 4, co. 2, Legge 3 agosto 2009, n.116, come sostituito dall'art. 2, co. 1, Decreto Legislativo 7 luglio 2011, n. 121, che ha inserito nel d.lgs. 231/2001 l'articolo 25-*undecies*;
 - **reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare**, introdotto dall'art. 2 del Decreto Legislativo 16 luglio 2012, n. 109, che ha inserito nel d.lgs. 231/2001 l'articolo 25-*duodecies*;
 - **reati transnazionali**, introdotti dalla Legge 16 marzo 2006 n. 146, “Legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale”, che vengono di seguito elencati:
 - reato di associazione per delinquere (articolo 416 c.p.);
 - reato di associazione di tipo mafioso (articolo 416 *bis* c.p.);
 - reato di associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (articolo 291 *quater* D.P.R. 23 gennaio 1973, n. 43);
 - reato di associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (articolo 74 D.P.R. 9 ottobre 1990, n. 309);
 - reato relativo al traffico di migranti (articolo 12, commi 3, 3 *bis*, 3 *ter* e 5 d.lgs. 25 luglio 1998, n. 286);
 - reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 377 *bis* c.p.)
 - reato di favoreggiamento personale (articolo 378 c.p.).

I presupposti normativi perché un ente possa incorrere nella descritta responsabilità risultano essere:

- a) che una persona fisica – che si trovi rispetto all'ente in una delle relazioni previste dall'art. 5 – commetta uno dei reati in questione;
- b) che il reato sia stato commesso nell'interesse o a vantaggio dell'ente (responsabilità oggettiva);
- c) che il reato commesso dai soggetti individuati dalla legge derivi quanto meno da una “colpa di organizzazione” dell'ente (responsabilità soggettiva).

Per quanto riguarda il primo aspetto, il D.Lgs. 231/01 individua all'art. 5 due tipologie di soggetti i quali, qualora dovessero commettere nell'interesse o a vantaggio dell'ente uno dei reati sopra evidenziati, possono determinare una responsabilità a carico dell'ente stesso.

¹ Il reato di “autoriciclaggio” è stato introdotto con la Legge 186 del 2014 ed è stato recepito nell'ambito dell'art 25 *octies* del D. Lgs 231 del 2001.

Secondo il dettato della citata norma, “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)”.

Tuttavia, “*l’ente non risponde se le persone indicate nel comma 1 hanno agito nell’interesse esclusivo proprio o di terzi*”.

La prima delle descritte figure parrebbe corrispondere, nella struttura societaria, a quella degli amministratori, dei direttori generali, dei preposti a sedi secondarie e, in caso di organizzazione divisionale, dei direttori di divisione.

“Soggetto all’altrui direzione” può invece essere chiunque si trovi ad operare nell’ente in una posizione anche non formalmente inquadrabile in un rapporto di lavoro dipendente, purché sottoposto alla direzione o alla vigilanza altrui.

La sola esistenza di uno dei rapporti descritti dall’art. 5 in capo all’autore del reato non basta di per sé a far sorgere la responsabilità dell’ente.

Infatti, occorre anche che il reato sia stato commesso nell’interesse o a vantaggio dell’ente medesimo.

Perciò, l’ente risponde del reato, sia che il suo autore lo abbia commesso con l’intenzione di perseguire un interesse (esclusivo o concorrente) dell’ente, sia che il reato si riveli comunque vantaggioso per l’ente medesimo. Tuttavia, la responsabilità dell’ente resta esclusa se risulta che l’autore del reato ha agito al fine di perseguire un interesse esclusivamente proprio o comunque diverso da quello dell’ente.

Perché possa configurarsi la responsabilità dell’ente, è comunque necessario che sussista una “colpa di organizzazione” da parte dell’ente stesso, da intendersi quale comportamento omissivo consistente nel non aver istituito un efficiente ed efficace sistema di prevenzione dei reati.

Gli artt. 6 e 7 del Decreto offrono infatti all’ente l’opportunità di una possibile esclusione della propria responsabilità², disciplinando le condizioni al verificarsi delle quali l’ente non risponde del reato commesso dai soggetti individuati nell’art. 5.

Introducendo un’inversione dell’onere della prova, l’art. 6 del D.lgs. 231/01 – rubricato “Soggetti in posizione apicale e modelli di organizzazione dell’ente” – prevede che “se il reato è stato commesso dalle persone indicate nell’articolo 5, comma 1, lettera a), l’ente non risponde se prova che:

- a) l’organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto,

² Va notato che l’adozione del Modello può servire – oltretutto ad escludere in radice la responsabilità dell’ente – se adottato prima dell’apertura del dibattimento, ad evitare all’ente l’applicazione delle più gravi sanzioni interdittive (art. 17, lett. b); a determinare una sensibile riduzione delle pene pecuniarie (art. 12, secondo comma, lett. b, e terzo comma).

Anche la semplice dichiarazione di voler predisporre ed attuare tali modelli, unitamente alle altre condizioni enunciate nel citato art. 17, può giustificare la sospensione delle misure cautelari interdittive eventualmente adottate in corso di causa (art. 49, primo comma); misure destinate poi ad essere del tutto revocate in caso di effettiva attuazione del modello e delle altre richiamate condizioni (art. 49, quarto comma; art. 50, primo comma).

Infine, l’adozione del Modello può avere luogo anche a sentenza di condanna già emessa, al fine di ottenere la conversione delle sanzioni interdittive (art. 78).

- modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
 - c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
 - d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)”.

Analogamente, il successivo art. 7 – rubricato “Soggetti sottoposti all'altrui direzione e modelli di organizzazione dell'ente” – statuisce che “nel caso previsto dall'articolo 5, comma 1, lettera b), l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza”.

1.3 L'adozione del “Modello” quale possibile esimente della responsabilità amministrativa

In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati di cui al Decreto.

Il Modello prevede, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

In particolare il Decreto agli articoli 6 e 7 prevede una forma di esonero della responsabilità qualora la società dimostri di aver adottato ed efficacemente attuato “modelli di organizzazione, gestione e controllo” idonei a prevenire la realizzazione degli illeciti considerati.

Ai fini di idoneità, i suddetti Modelli devono rispondere alle seguenti esigenze, “in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi i reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello”.

L'efficace attuazione del Modello richiede:

- a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni, ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;

- b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello, sia nei confronti dei soggetti apicali che dei soggetti sottoposti all'altrui direzione.

Va precisato che il D.Lgs. 231/2001 nonché il relativo Regolamento di attuazione emanato con D.M. 26 giugno 2003 n. 201, afferma che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, *“sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro trenta giorni, osservazioni sull'idoneità dei modelli a prevenire i reati?”*.

2. ADOZIONE DEL MODELLO IN TIP – TAMBURI INVESTMENT PARTNERS S.P.A.

2.1. Obiettivi perseguiti con l'adozione del Modello

Tamburi Investment Partners S.p.A. (di seguito anche la “Società” ovvero “TIP”), nell'intento di assicurare - a tutela della propria posizione e immagine - condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali ha ritenuto di procedere all'attuazione del modello di organizzazione, gestione e controllo di cui al Decreto Legislativo 231/2001.

Tale iniziativa è stata assunta nella convinzione che l'adozione di tale Modello - al di là delle previsioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio - possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano nella Società, affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di compimento dei reati contemplati nel Decreto.

La Società con delibera del Consiglio di Amministrazione del 9 marzo 2018 ha provveduto ad aggiornare il proprio modello di organizzazione, gestione e controllo (già precedentemente adottato), alla luce dei nuovi reati introdotti nel D.Lgs. 231/2001.

Il Modello fa riferimento al sistema strutturato e organico di norme, procedure operative ed informatiche e controlli in vigore in TIP idoneo a prevenire la commissione delle diverse tipologie di reato previste dal Decreto.

All'interno della normativa della Società una particolare rilevanza assume quella che regola le attività a rischio di reato ai sensi del D.Lgs. 231/2001 con particolare riferimento agli aspetti attinenti a:

- definizione di deleghe, poteri, norme per l'uso della firma sociale, ecc.;
- verificabilità e documentabilità delle operazioni;
- separatezza delle funzioni;
- effettuazione di controlli a diversi livelli.

Più in particolare, mediante l'individuazione delle attività “sensibili” a rischio di reato (cfr. Allegato 1 – Mappatura delle attività a rischio ex D.Lgs. 231/ 2001) e la conseguente regolamentazione, il Modello si propone come finalità quelle di:

- determinare, in tutti coloro che operano nelle aree in cui si effettuano attività “sensibili” la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti

- ma anche nei confronti dell'azienda;
- ribadire che tali forme di comportamento illecito sono fortemente condannate dalla Società in quanto (anche nel caso in cui essa fosse apparentemente in condizione di trarne vantaggio) contrarie, oltre che alle disposizioni di legge, anche ai principi etico / sociali cui TIP intende attenersi nell'assolvimento della propria missione;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle aree in cui vengono svolte attività "sensibili", di intervenire tempestivamente per prevenire o contrastare il compimento dei reati stessi.

Oltre ai principi sopra indicati, un efficace Modello presuppone:

- un'attività di sensibilizzazione e la diffusione a tutti i livelli aziendali di un'approfondita conoscenza delle regole comportamentali in vigore in TIP;
- la disponibilità della mappa, sempre aggiornata, delle attività "sensibili" ai sensi del Decreto e delle Strutture Aziendali in cui possono realizzarsi i reati in parola;
- l'attribuzione all'Organismo di Vigilanza di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello, nonché la messa a disposizione dell'Organismo di Vigilanza di risorse aziendali adeguate e proporzionate ai compiti affidatigli e ai risultati attesi e ragionevolmente attendibili;
- la verifica e la documentazione delle operazioni "sensibili";
- il rispetto del principio della separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico.

2.2 Adozione del Modello e costituzione dell'Organismo di Vigilanza

Il Modello viene adottato dal Consiglio di Amministrazione, il quale, sempre in attuazione di quanto previsto dal D. Lgs. 231/01, costituisce con delibera consiliare il proprio "Organismo di Vigilanza", che ha il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello e di supportare il processo di aggiornamento dello stesso.

2.3. La costruzione del Modello e la sua struttura

Al fine di procedere alla predisposizione del Modello di cui agli artt. 6 e 7 del Decreto, nonché alle successive attività di aggiornamento dello stesso, la Società ha avviato una serie di attività propedeutiche suddivise in differenti fasi, dirette alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D.Lgs. 231/2001 ed ispirate alle norme in esso contenute.

Innanzitutto sono state identificate le aree a rischio di reato.

L'attività di mappatura è stata svolta attraverso il censimento delle singole attività "a rischio" (in connessione con la tipologia di reato).

Sulla base delle analisi svolte si è quindi proceduto alla predisposizione del Modello e alla sua adozione, deliberata dal Consiglio di Amministrazione della Società.

Il modello di organizzazione, gestione e controllo si compone dei seguenti elementi:

- riferimenti normativi circa il Decreto Legislativo 231/2001;
- mappatura delle attività a rischio ed relativi presidi organizzativi in vigore;
- protocolli di controllo volti a prevenire la commissione dei reati rientranti nel novero del Decreto (ovvero disposizioni organizzative interne aventi la medesima finalità);
- Organismo di Vigilanza;
- flussi informativi e segnalazioni da/verso l'Organismo di Vigilanza;
- sistema disciplinare;
- Codice Etico.

che rappresentano il corpo centrale del presente documento.

L'attività di predisposizione del Modello è stata svolta attraverso i seguenti passi operativi:

- a) definizione della **metodologia** di mappatura delle attività a rischio di reato;
- b) definizione della mappa delle attività "sensibili" a rischio di reato e individuazione dei relativi presidi organizzativi di mitigazione del rischio (cfr. Allegato 1 - Mappatura delle attività a rischio ex D.Lgs. 231/ 2001).

L'attività è stata svolta attraverso raccolta e analisi della documentazione rilevante ai sensi del D.Lgs. 231/2001 e relativa ai presidi organizzativi in vigore, ed è stata successivamente verificata, completata e condivisa attraverso intervista con il Vice Presidente della Società, in particolare con l'obiettivo di:

- verificare l'esaustività dell'elenco delle attività sensibili;
- verificare la coerenza dei presidi di controllo già in vigore (es. procedure, istruzioni, sistemi di delega, elementi di sicurezza logica, etc.) volti a scoraggiare ovvero impedire i comportamenti illeciti;
- condividere le aree di miglioramento individuate (come gap rispetto ai controlli esistenti) e i piani di azione proposti a superamento dei suddetti gap, da realizzare attraverso l'integrazione della normativa in vigore, ovvero attraverso la predisposizione di normative speciali ad hoc.

La mappa è stata articolata come di seguito indicato:

- attività a rischio reato;
- reati potenziali;
- possibili modalità di commissione dei reati;
- strumenti di controllo esistenti;
- punti di miglioramento;
- piani d'azione;
- analisi del modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001.

Il Modello è stato prioritariamente definito nelle sue componenti fondamentali secondo le indicazioni di cui alle Linee Guida emanate Confindustria e conformemente alle migliori prassi di settore. Il Modello si compone dei seguenti elementi:

- Organismo di Vigilanza;
- definizione dei flussi informativi rivolti all'Organismo di Vigilanza;
- sistema disciplinare;
- Codice Etico.

Si riporta di seguito un dettaglio circa la descrizione e le finalità delle suddette componenti facenti parte del presente modello di organizzazione gestione e controllo.

3. L'ORGANISMO DI VIGILANZA

3.1 Composizione dell'Organismo di Vigilanza

Il Decreto identifica in un "organismo dell'ente", dotato di autonomi poteri di iniziativa e di controllo (art. 6, comma 1, lett. b), l'organo al quale deve essere affidato il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello nonché di curarne il costante e tempestivo aggiornamento.

La genericità del concetto di "organismo dell'ente" giustifica l'eterogeneità delle soluzioni che al riguardo possono adottarsi in considerazione sia delle proprie caratteristiche dimensionali, sia delle proprie regole di *corporate governance*, sia della necessità di realizzare un equo bilanciamento tra costi e benefici.

Indipendentemente dalla specifica composizione e struttura dell'Organismo di Vigilanza, resta fermo che esso debba ispirare la propria azione ai seguenti principi:

- a) attività di controllo sull'effettività del Modello;
- b) attività di vigilanza sull'adeguatezza del Modello;
- c) continuità di azione;

nonché debba avere caratteristiche quali:

- a) conoscenze di tecniche e strumenti adeguati (es. conoscenze legali, di gestione di rapporti con le risorse umane, ecc.);
- b) personale dedicato di adeguato spessore e consistenza;
- c) poteri di acquisizione e di richiesta di informazioni da e verso ogni livello e settore operativo della Società;
- d) possibilità di avviare procedimenti disciplinari e di proporre eventuali sanzioni a carico di soggetti che non abbiano rispettato le prescrizioni contenute nel modello di organizzazione, gestione e controllo;
- e) indipendenza da responsabilità di gestione aziendale e soprattutto di autonomia rispetto ai vertici aziendali.

L'Organismo di Vigilanza istituito dalla Società provvede autonomamente a disciplinare le regole per il proprio funzionamento, formalizzandole in apposito regolamento.

3.2. Durata in carica e sostituzione dei componenti

Il Consiglio d'Amministrazione provvede alla nomina dell'Organismo di Vigilanza mediante apposita delibera. È altresì rimessa all'Organo amministrativo la responsabilità di valutare periodicamente l'adeguatezza dell'Organismo di Vigilanza in termini di struttura organizzativa e di poteri conferiti, apportando, mediante delibera, le modifiche e/o integrazioni ritenute necessarie. In particolare:

- i componenti dell'Organismo non possono essere revocati dal Consiglio di Amministrazione se non per giustificato motivo;
- qualora venga a mancare, per dimissioni o altre cause, uno dei componenti dell'Organismo, e resti comunque in carica la maggioranza dei componenti dello stesso, il Consiglio, anche su

proposta del medesimo Organismo, potrà nominare un sostituto che resti in carica fino alla scadenza del mandato;

- l'Organismo si intende decaduto se vengono a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, il Consiglio di Amministrazione provvede a nominare i nuovi componenti.

3.3. Cause di ineleggibilità ed incompatibilità

Costituiscono cause di ineleggibilità e/o di decadenza dall'incarico dei membri dell'Organismo di Vigilanza:

- la condanna (o il patteggiamento), con sentenza anche non irrevocabile, per aver commesso uno dei reati previsti dal D.Lgs. 231/2001;
- la condanna, con sentenza passata in giudicato, a una pena che importa l'interdizione - anche temporanea - dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
- l'assenza ingiustificata da tre riunioni consecutive;
- l'applicazione di sanzioni disciplinari eccedenti il rimprovero verbale;
- le dimissioni volontarie dall'incarico.

I rappresentanti del Consiglio di Amministrazione - in particolare - non dovranno, inoltre essere titolari di poteri delegati dal Consiglio.

3.4 Funzioni e poteri dell'Organismo di Vigilanza

Con l'adozione del presente Modello e con la conseguente istituzione dell'Organismo di Vigilanza a quest'ultimo è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello medesimo e di curarne l'aggiornamento.

Premesso che la responsabilità ultima dell'adozione del Modello resta in capo al Consiglio d'Amministrazione, all'Organismo di Vigilanza è affidato il compito di vigilare con autonomi poteri di iniziativa e di controllo:

- sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati;
- sull'osservanza delle prescrizioni contenute nel presente documento da parte degli Organi Sociali, dei Dipendenti, delle Società di Service e degli altri soggetti terzi;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

Al fine dell'assolvimento dei compiti sopra riportati, l'Organismo di Vigilanza dovrà:

- con riferimento alla verifica dell'efficacia del Modello:
 - interpretare la normativa rilevante;
 - coordinare l'attività di determinazione degli standard e delle procedure atte a prevenire il verificarsi di condotte illecite ai sensi del Decreto;
 - coordinarsi con la funzione aziendale preposta per la definizione dei programmi di formazione per il personale e del contenuto delle comunicazioni periodiche da farsi agli Organi Sociali, ai Dipendenti e agli *Outsourver*, finalizzate a fornire agli stessi la necessaria

- sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001;
- monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello;
 - valutare l'adeguatezza del sistema dei controlli ai fini della prevenzione di comportamenti illeciti o in contrasto con il Modello;
 - predisporre ed aggiornare con continuità le informazioni rilevanti al fine di consentire una piena e consapevole adesione alle regole di condotta della Società. A tale fine l'Organismo di Vigilanza verificherà l'aggiornamento dello spazio Intranet della Società dedicato al Modello;
- con riferimento alla verifica dell'osservanza del Modello dovrà:
 - effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere dalla Società nell'ambito dei processi sensibili;
 - ricevere segnalazioni da parte del personale in merito ad eventuali anomalie;
 - coordinare eventuali investigazioni/inchieste finalizzate all'accertamento della coerenza tra i comportamenti concreti ed il Modello istituito;
 - raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere trasmesse o tenute a disposizione dell'Organismo stesso;
 - con riferimento alle proposte di aggiornamento del Modello e di monitoraggio della loro realizzazione:
 - sulla base delle risultanze emerse dalle attività di verifica e controllo, esprimere annualmente una valutazione sull'adeguatezza del Modello, rispetto alle prescrizioni del Decreto e all'operatività aziendale;
 - condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle attività "a rischio reato" e dei relativi processi sensibili;
 - in relazione a tali valutazioni, presentare periodicamente all'Organo Amministrativo apposita relazione;
 - verificare periodicamente l'attuazione ed effettiva funzionalità delle soluzioni/azioni correttive proposte;
 - coordinarsi con i responsabili delle competenti funzioni aziendali per valutare l'adozione di eventuali sanzioni disciplinari, ferma restando la competenza del competente Organo/funzione aziendale per l'irrogazione della sanzione e il relativo procedimento disciplinare.

Nell'espletamento di tali attività, l'OdV potrà avere accesso libero ed incondizionato ad informazioni, documenti ed ogni altro elemento ritenuto importante - ai fini dello svolgimento dei propri compiti - detenuto dalle diverse strutture della Società.

3.5 Reporting verso il Consiglio di Amministrazione

Per una piena aderenza ai dettami del Decreto, l'Organismo di Vigilanza riporta direttamente al Consiglio di Amministrazione, in modo da garantire la sua piena autonomia ed indipendenza nello svolgimento dei compiti che gli sono affidati.

Ferma restando la piena autonomia e indipendenza dell'Organismo di Vigilanza, per i compiti ad esso affidati quest'ultimo è tenuto a presentare una relazione scritta sugli esiti delle proprie attività al Consiglio di Amministrazione con periodicità almeno semestrale e comunque ogni volta che ve ne sia urgenza, o quando richiesto da un componente dell'Organismo di Vigilanza.

La relazione ha ad oggetto:

- l'attività svolta, indicando in particolare le verifiche condotte e l'esito delle stesse, l'eventuale aggiornamento delle attività "a rischio reato" e dei connessi processi sensibili;
- le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni, sia in termini di efficacia del Modello;
- gli interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione;
- la rendicontazione delle spese eventualmente sostenute a fronte dell'espletamento degli adempimenti di competenza dell'Organismo di Vigilanza.

Ogni anno l'Organismo di Vigilanza sottopone al Consiglio di Amministrazione un piano delle attività previste per l'anno successivo.

L'Organismo, anche tramite l'attività di Internal Audit, può rivolgere comunicazioni al Presidente del Consiglio d'Amministrazione o anche al Consiglio d'Amministrazione al Collegio Sindacale e alla società di revisione, i quali possono a loro volta richiederne al Presidente la convocazione di una riunione, in ogni circostanza in cui sia ritenuto necessario o opportuno per il corretto svolgimento delle proprie funzioni e per l'adempimento degli obblighi imposti dal Decreto.

Di eventuali apposite riunioni dell'Organismo di Vigilanza con gli organi sociali deve essere predisposto verbale. Copie dei relativi verbali devono essere custodite dall'Organismo di Vigilanza.

4. FLUSSI INFORMATIVI E SEGNALAZIONI VERSO L'ORGANISMO DI VIGILANZA

4.1 Flussi informativi nei confronti dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha il compito di monitorare tutte le operazioni potenzialmente sensibili e di predisporre un efficace sistema di comunicazione interna per consentire la trasmissione e raccolta di notizie rilevanti per il D. Lgs. 231/01.

A tal fine per ciascuna Area, sono state identificate alcune fattispecie di informazioni da inoltrare all'Organismo (cfr. Allegato 2 – Flussi informativi verso/ da l'Organismo di Vigilanza).

4.2 Segnalazioni all'Organismo di Vigilanza

Le segnalazioni verso l'Organismo di Vigilanza possono essere di varia natura e riguardare tanto violazioni, o presunte violazioni, quanto fatti, ordinari e straordinari, rilevanti ai fini della attuazione ed efficacia del Modello.

Obblighi di informativa relativi ad atti ufficiali

Devono essere trasmesse all'Organismo di Vigilanza le informative concernenti:

- le segnalazioni o le richieste di assistenza legale inoltrate dal personale in caso di avvio di procedimento giudiziario per uno dei reati previsti dal Decreto;
- le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate, in relazione a fattispecie previste dal D.Lgs. 231/01 ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

Segnalazioni di violazione del Modello

Chiunque (dipendente, collaboratore, ecc.), nello svolgimento della propria attività, venga a conoscenza di violazione o sospetti violazione delle regole previste dal modello di organizzazione, gestione e controllo deve effettuare segnalazione in forma scritta all'Organismo di Vigilanza.

Il soggetto segnalante dovrà utilizzare il "Modulo standard di segnalazione" (vedi Allegato 3) messo a disposizione. La segnalazione deve essere inviata al seguente indirizzo di posta elettronica: matteo.pagani@milano.pecavvocati.it.

Ciascuna segnalazione dovrà essere sufficientemente circostanziata e contenere informazioni sufficienti ad identificare i termini della violazione stessa al fine di permettere all'Organismo di Vigilanza di procedere tempestivamente ed in modo appropriato nelle attività di indagine.

L'Organismo di Vigilanza valuterà con tempestività le segnalazioni ricevute e gli eventuali provvedimenti conseguenti da promuovere. L'eventuale decisione di non dar corso all'effettuazione di indagini interne dovrà essere documentata e conservata.

E' compito dell'Organismo di Vigilanza promuovere l'attivazione di eventuali provvedimenti disciplinari in caso di accertate violazioni del Modello, anche in maniera indipendente dall'eventuale procedimento della magistratura.

L'Organismo di Vigilanza agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, il venir meno a tale obbligo rappresenta una grave violazione del Modello.

Gli obblighi di segnalazione da parte di dipendenti ed altri soggetti apicali dovranno trovare adeguata pubblicità nell'ambito delle consuete modalità di comunicazione interna. Gli obblighi di segnalazione da parte dei collaboratori esterni saranno specificate in apposite clausole inserite nei contratti che legano tali soggetti alla società.

5. SISTEMA DISCIPLINARE

5.1 Funzioni del sistema disciplinare

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del Decreto stabiliscono espressamente (con riferimento sia ai soggetti in posizione apicale sia ai soggetti sottoposti ad altrui direzione) che l'esonero da responsabilità dell'ente è subordinato, tra l'altro, alla prova dell'avvenuta introduzione di "un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello".

La definizione di un sistema di sanzioni commisurate alla gravità della violazione e con finalità deterrenti, concorre a rendere efficace l'azione di vigilanza dell'OdV ed a garantire l'effettiva osservanza del Modello.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria a carico dell'autore materiale della condotta criminosa.

5.2 Misure nei confronti di quadri ed impiegati

Violazioni

Fermi restando gli obblighi nascenti dalla legge 30 maggio 1970, n. 300 (c.d. "Statuto dei lavoratori") e dalle altre norme di legge applicabili, i comportamenti sanzionabili che costituiscono violazione del Modello sono di seguito esemplificativamente elencati, in ordine di gravità crescente:

- a) violazione di regole o di procedure interne adottate in attuazione del Modello o ivi contenute (ad es., omissione di comunicazioni o false comunicazioni all'OdV, ostacolo all'attività dell'OdV, omissione di controlli, ecc.);
- b) violazione di prescrizioni del Codice Etico;
- c) comportamenti diretti univocamente al compimento di uno o più reati, o comunque idonei ad esporre la Società alle conseguenze della commissione dei reati.

Le sanzioni verranno commisurate al livello di responsabilità ed autonomia operativa del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità e gravità del suo comportamento (misurabile in relazione al livello di rischio cui la Società è esposta).

Il sistema disciplinare è soggetto a costante verifica da parte dell'OdV e del Presidente di TIP, rimanendo quest'ultimo responsabile della concreta applicazione delle misure disciplinari qui delineate, su eventuale segnalazione dell'OdV.

Sanzioni

La violazione delle procedure, dei sistemi di controllo, del Codice Etico e del Modello da parte dei Dipendenti costituisce sempre illecito disciplinare. Pertanto: (i) ogni notizia di violazione determinerà l'avvio di un procedimento disciplinare; (ii) all'autore della violazione, debitamente accertata, verrà comminata una sanzione disciplinare; (iii) tale sanzione sarà proporzionata alla gravità dell'infrazione.

I provvedimenti disciplinari irrogabili nei riguardi dei Dipendenti – nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori e di altre norme eventualmente applicabili – sono previsti dal CCNL come segue:

- a) rimprovero verbale;
- b) rimprovero scritto;
- c) sospensione dal lavoro e dalla retribuzione fino a tre giorni;
- d) licenziamento con preavviso;
- e) licenziamento senza preavviso.

5.3 Misure nei confronti degli amministratori

In caso di mancata osservanza del Modello o del Codice Etico da parte di uno o più amministratori, l'OdV ne darà comunicazione immediata al Collegio Sindacale ed all'intero Consiglio di Amministrazione per l'adozione degli opportuni provvedimenti.

5.4. Misure nei confronti dei sindaci

In caso di mancata osservanza del Modello o del Codice Etico da parte di uno o più sindaci, l'OdV informerà l'intero Collegio Sindacale e il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti.

5.5 Misure nei confronti di consulenti e Partner

La mancata osservanza del Modello o del Codice Etico da parte di Consulenti o Partner, inseriti o richiamati da apposite clausole contrattuali, è sanzionata secondo quanto previsto in dette clausole, ed in ogni caso con l'applicazione di penali e/o l'automatica risoluzione del contratto, salvo il risarcimento del danno.

I Consulenti o i Partner non dovranno indurre i Dipendenti a violare il Codice Etico o il Modello.

6. REGOLE DI COMPORTAMENTO E CODICE ETICO

La Società provvede a predisporre apposite regole di condotta e un Codice Etico che costituiscono parte integrante del presente modello di organizzazione, gestione e controllo e della normativa aziendale. Le regole definite sono vincolanti per i comportamenti posti in essere da tutti i destinatari dello stesso - tenuti ad adottare una condotta conforme alle regole stabilite per prevenire il verificarsi dei reati previsti nel D.Lgs. 231/01 - e saranno suscettibili di modifiche e/o integrazione in ragione dell'evoluzione delle norme di legge oltre che delle mutate esigenze.

7. DIFFUSIONE E INFORMAZIONE SUL MODELLO

Ai fini dell'efficacia del presente Modello deve essere svolta un'adeguata attività di diffusione/informazione nei confronti di tutto il personale, per favorire la conoscenza di quanto stabilito dal Decreto e dal modello di organizzazione, gestione e controllo adottato nelle sue diverse componenti.

Tutto il personale deve essere informato sul contenuto del Decreto e sul modello di organizzazione, gestione e controllo tramite comunicazioni interne.

I documenti devono essere opportunamente aggiornati in relazione alle evoluzioni delle normative esterne e del Modello.

La diffusione del Modello è obbligatoria: deve pertanto essere rilevata attestazione di conoscenza (tramite verifica dello stato di presa visione della normativa).

Ai nuovi assunti viene consegnato un set informativo, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza. Tale set informativo dovrà contenere, oltre ai documenti di norma consegnati al neo-assunto, il modello di organizzazione, gestione e controllo e il D.Lgs. 231/2001. I dipendenti saranno tenuti a rilasciare alla Società una dichiarazione sottoscritta ove si attesti la ricezione del set informativo nonché la integrale conoscenza dei documenti allegati e l'impegno ad osservarne le prescrizioni.

E' inoltre necessario prevedere analogia informativa e pubblicità del Modello anche per i collaboratori esterni, secondo modalità differenziate in relazione alla possibilità di accesso alla normativa aziendale, piuttosto che attraverso consegna cartacea del presente Modello (fatta eccezione per i relativi allegati ad uso esclusivo del personale interno alla Società) e del Codice Etico (con ricevuta di presa visione) ed eventualmente distinguendo in relazione alla tipologia di rapporto contrattuale e alla tipologia di attività svolta in relazione ai rischi di reato presupposto del D.Lgs. 231/2001.

8. FORMAZIONE SUL MODELLO

Al fine di garantire l'effettiva conoscenza del Modello e sensibilizzare il personale sul rispetto della normativa e sull'osservanza dei principi e delle procedure/ protocolli di cui il Modello si compone, devono essere previste specifiche attività formative definite all'interno di apposito e organico **piano formativo**.

Il Piano formativo deve essere articolato, in relazione ai **contenuti** e alle **modalità di erogazione**, in funzione della qualifica dei **destinatari**, del livello di rischio associato alle attività da questi svolte, dell'aver o meno funzioni di rappresentanza della società.

La formazione deve prevedere i seguenti **contenuti**:

- una parte istituzionale avente ad oggetto la normativa di riferimento (D.Lgs. 231/2001 e reati presupposto) e il Modello ed il suo funzionamento;
- una parte speciale, che avendo a riferimento la mappatura delle attività sensibili, sia volta a diffondere la conoscenza dei reati, le fattispecie configurabili ed i presidi specifici delle aree di competenza degli operatori.

La formazione è obbligatoria: deve pertanto essere rilevata attestazione di frequenza dei corsi.

I contenuti formativi devono essere opportunamente aggiornati in relazione alle evoluzioni della normativa esterna e del modello di organizzazione, gestione e controllo, prevedendo nel caso di aggiornamento significativo (es. estensione della responsabilità amministrativa dell'ente a nuove tipologie di reati), le necessarie integrazioni ai supporti formativi assicurando l'obbligatorietà di fruizione degli stessi.

L'Organismo di Vigilanza si occupa di promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello da parte di tutto il personale.

Sarà cura dell'Organismo di Vigilanza verificare la completa attuazione del piano di formazione, raccogliere le evidenze relative alla effettiva partecipazione ai programmi di formazione e di conservarle

negli appositi archivi, nonché di effettuare controlli periodici sul grado di conoscenza da parte dei dipendenti del Decreto e del Modello.

Parte Speciale

9. FINALITÀ

La presente Parte Speciale ha la finalità di definire linee e principi di comportamento che tutti i Destinatari del Modello dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività svolte dalla Società e considerate a rischio, la commissione dei reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- a) indicare le regole che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- b) fornire all'Organismo di Vigilanza e alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello Organizzativo;
- Codice Etico;
- Protocolli operativi;
- Procedure interne;
- Procure e deleghe;
- Circolari attuative/dispositive;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

E', inoltre, espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

La Società, per consentire ai Destinatari un accesso diretto ad eventuali segnalazioni di violazioni del Modello e del Codice Etico, nonché per qualsiasi comunicazione dovessero ritenere opportuna ai fini di un controllo relativo alla *compliance* aziendale, ha previsto un indirizzo di posta elettronica (matteo.pagani@milano.pecavvocati.it), del quale è a conoscenza tutto il personale, in questo senso dimostrando un'attenzione particolare alle tematiche di etica e legalità.

In particolare devono essere segnalati, a titolo esemplificativo, casi riguardanti i reati societari (false comunicazioni sociali, aggio, corruzione tra privati), reati in materia di riciclaggio, reimpiego e autoriciclaggio, reati in materia di violazione del diritto d'autore, reati in materia di abusi di mercato (*insider trading* e *market manipulation*), reati informatici o di trattamento illecito dei dati, e comunque ogni altra azione illegale.

Tale sistema, seppur non esaustivo rispetto alle finalità perseguite dal presente Modello, costituisce un valido ausilio in termini di prevenzione delle condotte di reato.

La Società si è inoltre attivata per l'approvazione e introduzione di un regolamento interno idoneo a disciplinare il sistema di segnalazione delle violazioni conforme alle intervenute novità legislative (c.d. *whistleblowing*).

10. La Società: attività e Governance

Tamburi Investment Partners S.p.A. (di seguito anche “TIP” o la “Società”) è una *holding* di partecipazioni indipendente, quotata in borsa sul mercato italiano, segmento STAR - Società con Alti Requisiti.

TIP ha partecipazioni sia in società quotate, che in società non quotate.

TIP svolge un’attività di investimento focalizzata su medie aziende italiane, che esprimono delle “eccellenze” nel relativo settore con investimenti azionari di minoranza, in società, quotate e non quotate.

Attraverso la divisione Tamburi & Associati - T&A TIP fornisce inoltre assistenza in operazioni di finanza straordinaria.

L’organigramma societario introduce le seguenti figure apicali:

- **Presidente e Amministratore Delegato** - Giovanni Tamburi
- **Vice Presidente e Amministratore Delegato** - Alessandra Gritti
- **Direttore Generale** - Claudio Berretti

Ciascuna di queste figure ha mansioni specificate in apposite *job descriptions*, che ne delimitano le responsabilità.

La Società è soggetta a controlli interni ed esterni per la verifica del rispetto di processi. Tali controlli avvengono con cadenze predeterminate o annualmente, sulla base dell’oggetto su cui vertono.

In conformità all’art. 6 del Decreto, il sistema dei controlli interni di TIP, in relazione ai reati da prevenire, prevede:

- **protocolli operativi** specifici relativi alle attività sensibili, per programmare la formazione e l’attuazione delle decisioni della Società;
- l’individuazione di **modalità di gestione delle risorse finanziarie** idonee ad impedire la commissione di reati.

I protocolli e le procedure interne sono costantemente aggiornati, anche su proposta o segnalazione dell’Organismo di Vigilanza.

L’Organismo medesimo verifica che i protocolli e le procedure siano idonei al rispetto dei principi contenuti nel Modello e nel Codice Etico di TIP.

L’Organismo concorre a definire, con le funzioni aziendali interessate, le operazioni di carattere significativo alle quali si applicano le procedure ispirate ai principi del Modello.

Sono indici di significatività dell’operazione: il suo valore e la sua portata economica in riferimento all’attività della Società nel comparto interessato, la sua incidenza sui processi decisionali, la sua rilevanza rispetto alla ordinaria attività di impresa.

Sono ammesse, nei casi di particolare urgenza o in caso di impossibilità temporanea di rispetto dei protocolli e delle procedure, sotto la responsabilità di chi le attua, eventuali deroghe a quanto previsto

nella presente Parte speciale, nella formazione o nell'attuazione delle decisioni. In tale evenienza è inviata immediata informazione all'Organismo di Vigilanza e, in ogni caso, è richiesta la successiva ratifica da parte del soggetto competente.

11. CLASSIFICAZIONE DEI REATI PRESUPPOSTO IN RELAZIONE ALLE AREE E OPERAZIONI A RISCHIO

Nell'ambito delle attività svolte da TIP sono state individuate le seguenti fattispecie di reato presupposto in relazione a determinate attività sensibili.

11.1 I reati nei confronti della pubblica amministrazione – artt. 24 e 25 D.Lgs. n. 231/01

Con riferimento agli artt. 24 e 25 del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Truffa in danno dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.)

Il delitto si sostanzia nel compimento di una condotta fraudolenta, connotata da raggiri e artifici, attraverso la quale l'autore della condotta, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. In particolare, l'artificio consiste in un'alterazione della realtà esterna dissimulatrice dell'esistenza o simulatrice dell'inesistenza, che determina nel soggetto passivo una falsa percezione della realtà, inducendolo in errore.

Il raggio, invece, opera non sulla realtà materiale ma sulla psiche del soggetto, consistendo in un avvolgimento subdolo dell'altrui psiche, mediante un programma ingegnoso di parole o argomenti destinato a persuadere e orientare in modo fuorviante le rappresentazioni e le decisioni altrui.

La fattispecie che viene in considerazione ai sensi del D.lgs. n. 231/01, è la truffa commessa a danno dello Stato o di altro ente pubblico.

Corruzione per un atto d'ufficio (artt. 318 c.p.)

Il reato si configura quando il pubblico ufficiale, per compiere un atto del proprio ufficio, riceve per sé o per altri una retribuzione, in denaro o altra utilità, non dovuta ovvero ne accetta la promessa.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il reato si configura quando il pubblico ufficiale, per omettere, ritardare o per aver omesso o ritardato un atto del proprio ufficio, ovvero per compiere un atto contrario ai doveri d'ufficio, riceve per sé o per altri denaro o altra utilità ovvero ne accetta la promessa.

Circostanze aggravanti (art. 319bis c.p.)

Il fatto di cui all'art. 319 c.p. è aggravato se ha per oggetto il conferimento di pubblici impieghi o di stipendi o pensioni o ancora se è volto alla stipulazioni di contratti a cui sia interessata l'amministrazione cui appartiene il pubblico ufficiale.

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

Tale fattispecie si realizza se i fatti indicati negli artt. 318 e 319 c.p., sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

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

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

Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)

Le disposizioni dell'art. 319 c.p. si applicano anche se il fatto è commesso da persona incaricata di un pubblico servizio; quelle di cui all'art. 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio, quale definito dall'art. 358 c.p., ma solo qualora rivesta la qualità di pubblico impiegato.

Pene per il corruttore (art. 321 c.p.)

La norma estende l'applicazione delle pene previste dagli artt. 318, comma 1 - 319 - 319bis - 319ter - 320 (in relazione alle ipotesi degli artt. 318 e 319) c.p. anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o un'altra utilità.

Istigazione alla corruzione (art. 322 c.p.)

La fattispecie criminosa in esame contempla la condotta di chi offre o promette danaro o altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di pubblico servizio, che rivesta la qualità di pubblico impiegato, per indurlo a compiere un atto del suo ufficio, ovvero ad omettere o ritardare un atto del suo ufficio ovvero ancora a fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata.

Concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e degli Stati esteri (art. 322bis c.p.)

Le disposizioni degli artt. 317, 318, 319, 319ter, 321 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 altro ente pubblico o privato presso le Comunità europee che svolgono attività corrispondenti a quelle di 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 o incaricati di pubblico servizio.

Si applicano inoltre le disposizioni di cui agli artt. 321 e 322 c.p. quando il denaro o altra utilità siano dati, offerti o promessi:

- a persone indicate nel punto primo di cui sopra, assimilate ai pubblici ufficiali o incaricati di pubblico servizio;
- 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 [diversi da quelli dell'Unione Europea, N.d.R.] o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o altri un indebito vantaggio in operazioni economiche internazionali".

Nozione di pubblico ufficiale e di incaricato di pubblico servizio (artt. 357 e 358 c.p.)

Ai fini dell'applicazione dei sopra citati delitti, sono:

- **pubblici ufficiali** coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. E' pubblica la funzione amministrativa caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione e dal suo svolgersi per mezzo di poteri autorizzativi o certificativi;

- **incaricati di pubblico servizio** coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima (quali quelli autorizzativi e certificativi).

11.1.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, tra gli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare con riferimento al rischio di commissione dei reati contro la Pubblica Amministrazione, le seguenti **attività sensibili** per la Società:

- Gestione dei contenziosi giudiziali e stragiudiziali (es. accordi transattivi, contenzioso giuslavoristico, contenzioso tributario): si tratta delle attività relative alla gestione dei contenziosi civili, penali e amministrativi, attivi e passivi;
- Rapporti con l'Autorità Giudiziaria nell'ambito di procedimenti penali;
- Gestione degli adempimenti e delle comunicazioni con le Autorità Pubbliche di vigilanza;
- Selezione e gestione dei fornitori;
- Gestione dei clienti;
- Gestione dei rapporti con l'Amministrazione Finanziaria (es. predisposizione della dichiarazione dei redditi o dei sostituti di imposta);
- Richiesta, ottenimento e gestione dei rapporti con soggetti pubblicisticamente qualificati in occasione di conseguimento o rinnovo di abilitazioni, concessioni, autorizzazioni, certificazioni e licenze, comunque denominate, rilasciate per l'esercizio dell'attività di impresa;
- Gestione dei rapporti, anche in caso di ispezioni, con soggetti pubblicisticamente qualificati, con Autorità di Vigilanza e controllo in materia fiscale, tributaria, societaria e finanziaria, ambientale, previdenziale, sanitaria, di sicurezza e igiene sul lavoro, prevenzione degli infortuni sul lavoro e assistenziale in genere, di immigrazione, espatrio da parte di personale provenienti da altri paesi extracomunitari;
- Assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale del personale: si tratta delle attività di assunzione delle figure professionali necessarie allo svolgimento delle attività aziendali, nonché della loro gestione nelle ipotesi in cui il personale abbia intrattenuto recenti rapporti, a qualsiasi titolo, con la P.A. ovvero in caso di accesso all'impiego di ammortizzatori sociali e contributi sull'occupazione nonché in relazione a categorie protette;
- Selezione e gestione dei consulenti;
- Gestione delle situazioni di conflitto di interesse degli Amministratori.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza

eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.2 I delitti informatici e trattamento illecito dei dati – art. 24bis, D.Lgs. 231/01

Con riferimento all'art. 24bis del Decreto - inserito dall'art. 7, comma 1, L. 18 marzo 2008 di "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica", stipulata a Budapest il 23 novembre 2011 -, i reati presupposto della responsabilità amministrativa di TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

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

La fattispecie sanziona chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

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

Il reato punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un profitto o un danno, 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 idonee al predetto scopo.

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

La fattispecie è tesa a sanzionare chiunque si procura, produce, riproduce, importa, diffonde, comunica o consegna, o comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informativi, allo scopo di danneggiare un sistema informatico o telematico, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento

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

La norma sanziona chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe nonché chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni indicate.

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

La fattispecie è volta a colpire chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico ovvero intercorrenti tra più sistemi.

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

Il reato sanziona chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

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

La condotta sanzionata è identificata in chiunque, salvo che il fatto non costituisca più grave reato, mediante le condotte di cui all'art. 635bis 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.

11.2.1 Le attività sensibili ai fini del D.Lgs. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, tra gli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare con riferimento al rischio di commissione dei reati informatici le seguenti **attività sensibili** per la Società:

- Utilizzo dei sistemi informatici da parte degli Utenti;
- Utilizzo e gestione dei sistemi informatici da parte dell'Amministratore di Sistema e di utilizzatori di *pc Administrator* oppure Utenti con accessi o permessi privilegiati;
- Utilizzo della firma digitale;
- Utilizzo della posta certificata;
- Smarrimento di strumenti informatici (pc portatile, *tablet*, telefoni cellulari, e simili).

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.2.2 I presupposti ai protocolli di prevenzione

Al fine di gestire in maniera esauriente i rischi identificati nell'ambito delle attività sensibili, è necessario che la Società dia applicazione alle previsioni indicate dal Regolamento Europeo n. 2016/679 in tema di protezione dei dati personali, in vigore dal 25 maggio 2016 ed in attuazione dal 25 maggio 2018.

Tali adempimenti si pongono quale presupposto indefettibile per la corretta identificazione e applicazione dei protocolli individuati di seguito.

11.2.2.1 Pianificazione

Preliminarmente, nell'ambito delle attività sensibili individuate, è opportuno fare anche riferimento ai documenti indicati dal D.lgs. n. 196/2003 e comunque alle norme che lo richiamano ovvero che ne fanno rinvio. Di seguito, in particolare, seppur con intenti non esaustivi, si richiamano:

- Modello Organizzativo Privacy (*ex* DPS);
- Codice Etico informatico/Politica sull'uso di internet;
- Predisposizione e organizzazione dell'organigramma della sicurezza informatica e le relative formalizzazioni di incarichi interni ed esterni;
- Applicazione di protocolli e procedure specifiche;
- Programmazione dei programmi di informazione e formazione.

11.2.2.2 Il Modello Organizzativo Privacy

Politica e Obiettivi: è necessaria l'esistenza di un documento (c.d. Modello Organizzativo Privacy) che formalizzi gli adempimenti in ambito trattamento dati personali, e in particolare che documenti l'adozione delle misure minime di sicurezza specificate dall'Allegato B al Codice Privacy (ovvero il Disciplinare tecnico in materia di dati personali). Tali misure minime di sicurezza sono applicate anche sui sistemi informatici che non supportano trattamenti di dati personali. Modello Organizzativo Privacy, inoltre, prevede:

- l'individuazione del trattamento del dato;
- l'individuazione degli applicativi informatici e cartacei utilizzati per la trattazione del dato;
- il censimento degli strumenti informatici volti al trattamento del dato;
- il censimento dei soggetti qualificati ai trattamenti dei dati (Incaricati);
- l'individuazione delle misure informatiche atte a proteggere il dato:
 - gestione delle *password*;
 - utilizzo dei supporti magnetici;
 - utilizzo dei pc portatili;
 - uso della posta elettronica;
 - uso della rete Internet e dei relativi servizi;
 - *policy* in materia di *privacy* e riservatezza del *know-how*.
- l'individuazione delle misure fisiche atte a proteggere il dato trattato;
- l'individuazione dei Responsabili interni;
- l'individuazione dei Responsabili esterni;
- l'individuazione degli archivi fisici e dei relativi accessi.

Prescrizioni legali e altre: è necessaria l'esistenza di una normativa aziendale che definisca criteri e modalità da adottare per:

- l'aggiornamento in relazione alla legislazione rilevante e alle altre prescrizioni applicabili in tema di sicurezza informatica (D.lgs. n. 196/2003);
- l'individuazione dell'ambito di applicazione di tali prescrizione (area aziendale) e le modalità di diffusione delle stesse.

11.2.2.3 Predisposizione e organizzazione dell'organigramma della sicurezza informatica e le relative formalizzazioni di incarichi interni ed esterni

La Società ha articolato la propria organizzazione aziendale per la sicurezza informatica con le figure previste dal D.lgs. n. 196/2003 e di seguito indicate:

- Titolare: con delibere del Consiglio di Amministrazione;
- Responsabile/i del/i Trattamento/i (artt. 4 e 29, D.lgs. n. 196/03): con delibera del Consiglio di Amministrazione;
- Incaricati: con atto di nomina espressa;
- Amministratore di Sistema: con atto di nomina formale;
- Responsabili Esterni: con nomina formale.

Tutte le figure del sistema sicurezza informatica sono individuate tramite procure, deleghe e nomine formali al fine della chiara attribuzione di funzioni e responsabilità nonché acquisizione di consapevolezza del proprio ruolo da parte dei questi, per permettere una definizione analitica del cd. "organigramma della sicurezza informatica".

Con delibera del Consiglio di Amministrazione è stata identificata l'Azienda quale Titolare, anche per la gestione di tutte le problematiche specifiche per la sicurezza informatica.

Le deleghe e le nomine sono rese note all'interno dell'organizzazione tramite comunicazioni organizzative.

Quanto all'organizzazione e alle responsabilità, sono stabilite:

- ◆ disposizioni organizzative per l'individuazione della figura di riferimento all'interno delle procedure informatiche, quale, ad esempio, il Responsabile del trattamento con i requisiti/doveri previsti e imposti dagli artt. 4 e 29 del D.lgs. n. 196/03, che si aggiunge e si alterna, nella responsabilità, al Titolare obbligatorio per il D.lgs. n. 196/03;
- ◆ disposizioni organizzative per l'individuazione delle regole e procedure per la gestione e il trattamento dei dati sia cartacei che informatici;
- ◆ la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti specifici previsti dalla normativa in materia Modello di Organizzazione, Gestione e Controllo (ex D.lgs. n. 231/01).

11.2.2.4 Applicazione di protocolli e procedure specifiche

Politica e Obiettivi: è necessaria l'esistenza di uno o più documenti che definiscano gli indirizzi e gli obiettivi generali specifici che l'azienda stabilisce di raggiungere. Gli stessi devono essere approvati dal

Titolare e resi noti all'Organismo di Vigilanza per le verifiche necessarie.

Detti documenti, inoltre, possono prevedere:

- procedure operative informatiche;
- istruzioni operative informatiche.

Prescrizioni legali e altre: è necessaria l'esistenza di una normativa aziendale che definisca criteri e modalità da adottarsi per:

- l'aggiornamento in relazione alla legislazione rilevante e alle altre prescrizioni applicabili in tema di sicurezza (D.lgs. n. 196/2003);
- l'individuazione dell'ambito di applicazione di tali prescrizioni (area aziendale) e le modalità di diffusione delle stesse.

11.2.2.5 La programmazione dei programmi di informazione e formazione

Politica e Obiettivi: è necessaria l'esistenza di un documento che definisca gli indirizzi e gli obiettivi generali specifici in tema di informazione e formazione in ambito di sicurezza informatica che l'azienda stabilisce di raggiungere con proiezione anche a 12 mesi. Lo stesso deve essere approvato dal Titolare e reso noto all'Organismo di Vigilanza per le verifiche necessarie.

Detto documento, inoltre, deve prevedere:

- la specifica dei corsi;
- il programma da tenere;
- la qualificazione del formatore;
- la durata degli stessi;
- il superamento di prove di apprendimento o addestramento;
- il rilascio degli attestati e delle certificazioni del caso;
- la periodicità e i criteri di aggiornamento.

Prescrizioni legali e altre: è necessaria l'esistenza di una normativa aziendale che definisca criteri e modalità da adottarsi per:

- l'aggiornamento in relazione alla legislazione rilevante e alle altre prescrizioni applicabili in tema di sicurezza (D.lgs. n. 196/2003);
- l'individuazione dell'ambito di applicazione di tali prescrizioni (area aziendale) e le modalità di diffusione delle stesse.

11.2.2.6 Il Controllo e le azioni correttive

Sono individuate attività volte ad implementare modalità di controllo del trattamento dei dati, nella accezione più ampia, garantendo altresì la misura e il monitoraggio degli stessi, potendo prevedere, implementare e attuare azioni correttive e preventive, modalità di gestione delle registrazioni, modalità di esecuzione, *audit* periodici.

Misura e monitoraggio degli accessi: è necessaria l'esistenza di una norma aziendale che indichi:

- le modalità di tracciamento, segnalazione, rilevazione, investigazione interna degli accessi

- informatici;
- i doveri di sovrintendere e vigilare sull’osservanza da parte dei singoli Incaricati dei rispettivi obblighi di legge, nonché delle disposizioni aziendali in materia di sicurezza informatica; di verificare affinché soltanto i lavoratori che abbiano ricevuto adeguate istruzioni accedano alle zone che li espongono a un rischio grave e specifico.

11.2.2.7 I piani di miglioramento

Periodicamente, anche sulla base delle eventuali segnalazioni ricevute, il Responsabile del trattamento, di concerto con il Titolare e con l’Amministratore di Sistema, individua e valuta se le misure di sicurezza informatica sono efficaci, le riesamina e programma eventuali integrazioni o aggiornamenti.

Gli obiettivi volti a rendere più efficace il sistema di sicurezza informatica vengono realizzati, mediante interventi integrativi sui protocolli e sulle procedure specifiche, sugli interventi formativi e sugli adeguamenti tecnologici tenuto conto dell’evoluzione scientifica.

11.3 I delitti di criminalità organizzata – art. 24^{ter}, D.Lgs. n. 231/01

L’art. 24^{ter} del Decreto introduce, ai fini della responsabilità dell’ente, i delitti di criminalità organizzata.

In proposito si richiama anche la L. n. 146 del 16 marzo 2006, che ha ratificato e dato esecuzione alla Convenzione e ai Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall’Assemblea Generale il 15 novembre 2000 e il 31 maggio 2001 (di seguito “Convenzione”).

La Convenzione si prefigge lo scopo di promuovere la cooperazione per prevenire e combattere il crimine organizzato transnazionale in maniera più efficace, richiedendo che ogni Stato parte della Convenzione adotti le misure necessarie, conformemente ai suoi principi giuridici, per determinare la responsabilità degli enti e delle società per i fatti di reato indicati dalla Convenzione stessa.

L’art. 10 della legge sopra menzionata prevede l’estensione della disciplina del Decreto con riferimento ad alcuni reati, ove ricorrano le condizioni di cui all’art. 3, ossia ove il reato possa considerarsi transnazionale.

L’art. 10 della Convenzione rubricato nella “Responsabilità delle persone giuridiche” così recita:

- 1) *“Ogni Stato adotta misure necessarie, conformemente ai suoi principi giuridici, per determinare le responsabilità delle persone giuridiche che partecipano a reati gravi che coinvolgono un gruppo criminale organizzato e per i reati di cui agli artt. 5, 6, 8 e 23 della presente Convenzione.*
- 2) *Fatti salvi i principi giuridici generali la responsabilità delle persone giuridiche può essere penale, civile o amministrativa.*
- 3) *Tale responsabilità è senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso i reati.*
- 4) *Ogni Stato Parte si assicura, in particolare, che le persone giuridiche ritenute responsabili ai sensi del presente articolo siano soggette a sanzioni efficaci, proporzionate e dissuasive, di natura penale o non penale, comprese sanzioni pecuniarie”.*

Per *Gruppo criminale organizzato*, ai sensi della Convenzione, si intende *un gruppo strutturato, esistente per un periodo di tempo, composto da tre a più persone che agiscono di concetto al fine di commettere uno o più reati gravi o reati stabiliti dalla convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale.*

Pertanto, con riferimento all'art. 24^{ter} del Decreto, i reati presupposto della responsabilità amministrativa di TIP, anche con riferimento alle previsioni dell'art. 10 della L. n. 146/06, possono essere identificati nelle seguenti fattispecie criminose:

Associazione per delinquere (art. 416 c.p.), anche transnazionale

La fattispecie si realizza quando tre o più persone si associano allo scopo di commettere più delitti.

Associazione di tipo mafioso (art. 416bis c.p.), anche transnazionale

Il codice sanziona il reato in esame, prevedendo che l'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono 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 e per realizzare profitti o vantaggi ingiusti per se o per altri, ovvero al fine di impedire o di ostacolare il libero esercizio del voto o di procurare vantaggio a sé o ad altri in occasione di consultazioni elettorali.

La condotta menzionata è richiamata dal decreto anche nelle ipotesi in cui assuma il carattere di transnazionalità, così come in questa sede identificato.

Scambio elettorale politico-mafioso (art. 416ter c.p.)

La fattispecie in esame sanziona chi ottiene la promessa di voti, secondo le modalità richiamate dall'art. 416bis, in cambio di erogazioni in danaro.

11.3.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, tra gli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto. Le analisi svolte hanno permesso di individuare con riferimento al rischio di commissione dei reati di criminalità organizzata, le seguenti **attività sensibili** per la Società:

- Gestione dei contenziosi giudiziali e stragiudiziali (es. accordi transattivi, contenzioso giuslavoristico, contenzioso tributario);
- Rapporti con l'Autorità Giudiziaria nell'ambito di procedimenti penali;
- Gestione dei rapporti con l'Amministrazione Finanziaria (es. predisposizione della dichiarazione dei redditi o dei sostituti di imposta);
- Gestione degli adempimenti e delle comunicazioni con le Autorità pubbliche di vigilanza;
- Gestione dei rapporti, anche in caso di ispezioni, con soggetti pubblicisticamente qualificati, con Autorità di Vigilanza e controllo in materia fiscale, tributaria, societaria e finanziaria, ambientale, previdenziale, sanitaria, di sicurezza e igiene sul lavoro, prevenzione degli infortuni sul lavoro e assistenziale in genere, di immigrazione, espatrio da parte di personale proveniente da paesi

- extracomunitari;
- Richiesta, ottenimento e gestione dei rapporti con soggetti pubblicisticamente qualificati in occasione del conseguimento o rinnovo di abilitazioni, concessioni, autorizzazioni, certificazioni e licenze, comunque denominate, rilasciate per l'esercizio dell'attività di impresa;
 - Gestione della clientela;
 - Selezione e gestione dei fornitori;
 - Selezione e gestione dei consulenti;
 - Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale;
 - Utilizzo dei sistemi informatici da parte degli Utenti;
 - Utilizzo e gestione dei sistemi informatici da parte dell'Amministratore di Sistema e di Utilizzatori di pc Administrator oppure Utenti con accessi/permessi privilegiati;
 - Gestione dei rapporti con il Collegio Sindacale e con la Società di revisione (*Auditor*);
 - Gestione delle situazioni di conflitto di interesse degli Amministratori;
 - Gestione dei prodotti e rifiuti, compilazione dei registri di controllo e flussi informativi verso le Autorità di Vigilanza.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.4 I reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento – art. 25bis, D.Lgs. n. 231/01

Con riferimento all'25bis del Decreto, si ritiene che le attività poste in essere da TIP non comportino il rischio di commissione dei reati presupposto previsti dalla norma.

11.5 I delitti contro l'industria e il commercio – art. 25bis.1, D.Lgs. n. 231/01

Con riferimento all'25bis.1 del Decreto, si ritiene che le attività poste in essere da TIP non comportino il rischio di commissione dei reati presupposto previsti dalla norma.

11.6 I reati societari – art. 25ter, D.Lgs. n. 231/01

Con riferimento all'art. 25ter del Decreto, i reati presupposto della responsabilità amministrativa TIP

possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

False comunicazioni sociali (art. 2621 c.c.)

Questo reato si realizza nel caso in cui amministratori, direttori generali, dirigenti preposti alla redazione dei libri contabili, sindaci e liquidatori, al fine di conseguire per sé o per altri un ingiusto profitto, espongono consapevolmente nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali rilevanti non rispondenti al vero, ovvero omettono dati materiali rilevanti la cui comunicazione è prevista dalla legge sulla situazione economica, patrimoniale o finanziaria della società. La condotta deve essere idonea ad indurre concretamente altri in errore e la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Fatti di lieve entità (art. 2621 bis c.c.)

La norma attenua le sanzioni nei casi di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta ovvero nei casi in cui i fatti riguardano società che non superano i limiti indicati dal secondo comma dell'art. 1 del R.D. 16 marzo 1942, n. 267. In tal caso, il delitto diviene procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

False comunicazioni sociali delle società quotate (art. 2622 c.c.)

Questo reato si realizza nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, 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 consapevolmente espongono fatti materiali 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.

A tali società sono equiparate:

- 1) le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
- 2) le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;
- 3) le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
- 4) le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Questa disciplina si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.)

La norma sanziona la condotta dei responsabili della revisione i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo a indurre in errore i destinatari delle comunicazioni sulla predetta

situazione.

Impedito controllo (art. 2625 c.c.)

Il reato consiste nella condotta degli amministratori di impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.

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

La condotta tipica prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, da parte degli amministratori, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)

Il reato prevede la condotta degli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva ovvero 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.

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

La fattispecie sanziona la condotta degli amministratori, che, fuori dai casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione dell'integrità del capitale sociale o delle riserve non distribuibili per legge ovvero, fuori dai 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.

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

La fattispecie si realizza quando gli amministratori effettuano, in violazione delle disposizioni di legge a tutela dei creditori, riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

Omessa comunicazione del conflitto di interessi (art. 2629bis c.c.)

La fattispecie consiste nell'omessa comunicazione da parte dell'amministratore, del componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al D.lgs. 24 febbraio 1998, n. 58 e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al D.lgs. 1 settembre 1993, n. 385, del citato testo unico di cui al D.lgs. n. 58 del 1998, del D.lgs. 7 settembre 2005, n. 209 o del D.lgs. 21 aprile 1993, n. 124, di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società.

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

Tale reato si consuma quando gli amministratori e i soci conferenti, 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.

Corruzione tra privati (art. 2635 c.c.)

La fattispecie si realizza quando gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati, - o chi, nell'ambito organizzativo della società o dell'ente privato, esercita funzioni direttive diverse da quelle proprie di questi soggetti - anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

E' punito, altresì, chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone suindicate.

La pena è ridotta se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti suindicati.

Le pene sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 TUF, di cui al D.lgs. 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nell'acquisizione di beni o servizi.

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

La fattispecie si realizza quando chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà e l'offerta o la promessa non sia accettata.

Sono puniti, altresì, gli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

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

Il reato punisce chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

Aggiotaggio (art. 2637 c.c.)

La fattispecie sanziona 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.

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

Il reato prevede la sanzione per gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i 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 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. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. Sono ancora puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, che, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

11.6.1 Le attività sensibili ai fini del D.Lgs. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati societari, le **attività sensibili**, di seguito elencate.

- Gestione dei contenziosi giudiziali e stragiudiziali (es. accordi transattivi, contenzioso giuslavoristico, contenzioso tributario);
- Predisposizione di bilanci, relazioni e comunicazioni sociali in genere;
- Gestione della clientela;
- Selezione e gestione dei fornitori;
- Selezione e gestione dei consulenti;
- Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale;
- Gestione di doni e regalie ricevuti dai dipendenti;
- Gestione dei rapporti con il Collegio Sindacale e con la Società di revisione (*Auditor*);
- Gestione delle situazioni di conflitto di interesse degli Amministratori;
- Gestione dei prodotti e rifiuti, compilazione dei registri di controllo e flussi informativi verso le Autorità di Vigilanza.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;

- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.7 I delitti con finalità di terrorismo o di eversione dell'ordine democratico – art. 25^{quater}, D.Lgs. n. 231/01

I delitti richiamati dall'art. 25^{quater} del Decreto sono da individuarsi in quelle fattispecie richiamate dal codice penale e dalle leggi speciali nonché gli altri delitti che siano comunque posti in essere in violazione di quanto previsto dalla Convenzione internazionale per la repressione del finanziamento del terrorismo, firmata a New York il 9 dicembre 1999. La Convenzione rinvia ai reati diretti a fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di terrorismo, richiamando altre convenzioni che riportano, nello specifico, dirottamento di aeromobili, attentati contro personale diplomatico, sequestro di ostaggi, illecita realizzazione di ordigni nucleari, dirottamento di navi, esplosione di ordigni, ecc.

Con riferimento a tale norma i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Associazione con finalità di terrorismo e di eversione dell'ordine democratico (art. 270 bis c.p.)

La norma riconosce la penale responsabilità in capo al soggetto che promuove, costituisce, organizza o dirige associazioni aventi quale compito atti di violenza con fini di eversione dell'ordine democratico, sanzionando anche la mera partecipazione.

11.7.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare con riferimento al rischio di commissione dei reati con finalità di terrorismo o eversione dell'ordine democratico le seguenti **attività sensibili** per la Società:

- Gestione della clientela;
- Selezione e gestione dei fornitori
- Selezione e gestione dei consulenti.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **oggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.8 I delitti contro la persona – artt. 25^{quater}.1 – 25^{quinquies}, D.Lgs. n. 231/01

Con riferimento agli artt. 25^{quater}.1 - 25^{quinquies} del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Riduzione o mantenimento in schiavitù (art. 600 c.p.)

La fattispecie richiama la condotta di chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce una persona in uno stato di soggezione continua, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento. La riduzione o il mantenimento nello stato di soggezione si verificano quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittando di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

Pornografia virtuale (art. 600^{quater}.1 c.p.)

La norma è tesa a colpire la condotta di chiunque ponga in essere i reati pornografia minorile e detenzione di materiale pornografico con riferimento a materiale pornografico rappresentato da immagini virtuali, ossia realizzate con tecniche di elaborazione in tutto o in parte associate a situazioni reali, la cui qualità faccia apparire come vere situazioni non reali, realizzate utilizzando minori di diciotto anni.

Tratta di persone (art. 601 c.p.)

La fattispecie punisce chiunque recluti, introduca nel territorio dello Stato, trasferisca anche al di fuori di esso, trasporti, ceda l'autorità sulla persona, ospiti una o più persone che si trovano in condizioni di schiavitù (ai sensi dell'art. 600 c.p.), ovvero, realizzi le stesse condotte su una o più persone, mediante inganno, violenza, minaccia, abuso di autorità o approfittamento di una situazione di vulnerabilità, di inferiorità fisica, psichica o di necessità, o mediante promessa o dazione di denaro o di altri vantaggi alla persona che su di essa ha autorità, al fine di indurle o costringerle a prestazioni lavorative, sessuali ovvero all'accattonaggio o comunque al compimento di attività illecite che ne comportino lo sfruttamento o il sottoporsi al prelievo di organi.

E' punito, altresì, chiunque, anche al di fuori delle modalità di cui sopra, realizzi tali condotte nei confronti di persona minore di età.

Alienazione ed acquisto di schiavi (art. 602 c.p.)

La disposizione si riferisce a chiunque, fuori dei casi indicati nell'art. 601, acquisti o alieni o ceda una persona che si trova in una delle condizioni di cui all'art. 600 c.p.

Intermediazione illecita e sfruttamento del lavoro - cd. Caporalato - (art. 603^{bis} c.p.)

La norma punisce, salvo che il fatto costituisca più grave reato, chiunque:

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

2) utilizzi, assunta o impieghi manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento e approfittando del loro stato di bisogno.

Se i fatti sono commessi mediante violenza o minaccia, la pena è aumentata.

Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;

2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;

3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;

4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Costituiscono aggravante specifica:

1) il fatto che il numero di lavoratori reclutati sia superiore a tre;

2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;

3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

Adescamento di minorenni (art. 609undecies c.p.)

La norma punisce chiunque, allo scopo di commettere i reati di cui agli art. 600 - 600bis - 600ter - 600quater c.p., anche se relativi al materiale pornografico di cui all'articolo 600quater.1 - 600quinquies - 609bis - 609quater - 609quinquies - 609octies c.p., adeschi un minore di anni sedici. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione.

11.8.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica tra gli elementi essenziali dei Modelli di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare con riferimento al rischio di commissione dei reati contro la persona le seguenti **attività sensibili** per la Società:

- Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale;
- Utilizzo dei sistemi informatici da parte degli Utenti;
- Utilizzo e gestione dei sistemi informatici da parte dell'Amministratore di Sistema e di Utilizzatori di pc Administrator oppure Utenti con accessi/permessi privilegiati.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e**

contrasto dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.9 Gli abusi di mercato – art. 25^{sexies}, D.Lgs. n. 231/01

Con riferimento all'art. 25^{sexies} del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Abuso di informazioni privilegiate (art. 184, D.lgs. n. 58/1998)

La norma punisce chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

- a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
- b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
- c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

E' punito, altresì, chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni suindicate.

La pena può essere aggravata quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

E' punita, altresì, la condotta suddetta quando ha ad oggetto operazioni relative agli strumenti finanziari di cui all'art. 180, comma 1, lettera a), numero 2).

Ai fini del presente articolo per strumenti finanziari si intendono anche gli strumenti finanziari di cui all'art. 1, comma 2, il cui valore dipende da uno strumento finanziario di cui all'art. 180, comma 1, lettera a).

Manipolazione del mercato (art. 185, D.lgs. n. 58/1998)

La norma punisce chiunque diffonda notizie false o ponga in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

La pena può essere aggravata quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

E' punita, altresì, la condotta suddetta quando ha ad oggetto gli strumenti finanziari di cui all'art. 180, comma 1, lettera a), numero 2).

11.9.1 Le attività sensibili ai fini del D.Lgs. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica tra gli elementi essenziali dei Modelli di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare con riferimento al rischio di commissione di abusi di mercato le seguenti **attività sensibili** per la Società:

- Gestione della clientela;
- Gestione delle cd. informazioni privilegiate (*Market abuse*);
- Utilizzo dei sistemi informatici da parte degli Utenti;
- Utilizzo e gestione dei sistemi informatici da parte dell'Amministratore di Sistema e di Utilizzatori di pc Administrator oppure Utenti con accessi/permessi privilegiati;
- Utilizzo della posta certificata.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **oggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.10 I reati in ambito di igiene e sicurezza sul lavoro – art. 25^{septies}, D.Lgs. n. 231/01

La L. 3 agosto 2007, n. 123, ha inserito nel D.lgs. n. 231/01 l'art. 25^{septies}, estendendo la responsabilità dell'ente ai reati di omicidio colposo e lesioni colpose gravi e gravissime commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro.

Il Consiglio dei Ministri in data 1 aprile 2008 ha approvato il D.lgs. n. 81/2008, attuativo della delega di cui all'art. 1 della L. 3 agosto 2007, n. 123 in materia di tutela della salute e sicurezza nei luoghi di lavoro.

Con riferimento all'art. 25^{septies} del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Omicidio colposo (art. 589 c.p.)

La fattispecie in esame si realizza quando si cagiona per colpa la morte di una persona con violazione delle norme per la prevenzione degli infortuni sul lavoro.

Lesioni colpose gravi o gravissime (art. 590, comma 3 c.p.)

La fattispecie in esame si realizza quando si cagiona ad altri per colpa una lesione personale grave o gravissima con violazione delle norme per la prevenzione degli infortuni sul lavoro.

Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro a che abbiano determinato una malattia professionale, è perseguibile d'ufficio.

La lesione personale è grave se dal fatto deriva una malattia che mette in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni o ancora se il fatto produce l'indebolimento permanente di un senso o di un organo; è gravissima se dal fatto deriva certamente una malattia certamente o probabilmente insanabile ovvero la perdita di un senso, arto o una mutilazione che renda l'arto inservibile, o ancora la perdita dell'uso di un organo o della capacità di procreare, una permanente e grave difficoltà della favella, la deformazione o lo sfregio permanente del viso.

11.10.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica tra gli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui all'art. 25^{septies} del Decreto, le seguenti **attività sensibili** della Società:

- Utilizzo prolungato di apparecchiature videoterminali;
- Movimentazione manuale e meccanica di pacchi inerenti l'approvvigionamento della cancelleria;
- Sostituzione e smaltimento degli inchiostri per stampanti;
- Esposizione prolungata al fumo passivo.

Per tali attività sensibili è stato predisposto un **protocollo operativo** per l'attività di "Sicurezza e prevenzione" (allegato al Modello) in cui sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.11 I reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché auto riciclaggio – art. 25^{octies}, d.Lgs. n. 231/01

Con riferimento all'art. 25^{octies} del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Ricettazione (art. 648 c.p.)

La norma punisce chi, fuori dei casi di concorso nel reato (art. 110 c.p.), 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. La pena è aumentata quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata ai sensi dell'art. 628, comma 3, c.p. di estorsione aggravata ai sensi dell'art. 629, comma 2, c.p. ovvero di furto aggravato ai sensi dell'art. 625, comma 1, n. 7^{bis}), c.p.

La pena è ridotta se il fatto è di particolare tenuità.

La norma si applica anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

Riciclaggio (art. 648^{bis} c.p.)

La disposizione è tesa a comminare una sanzione, fuori dei casi di concorso nel reato, nei confronti di chiunque sostituisca o trasferisca denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa

Impiego di denaro, beni o utilità di provenienza illecita (art. 648^{ter} c.p.)

La norma punisce chiunque, fuori dalle ipotesi di concorso nel reato e nei casi di riciclaggio o ricettazione, impieghi in attività economiche o finanziarie, denaro, beni o altre utilità provenienti da delitto.

Autoriciclaggio (art. 648^{ter.1} c.p.)

La norma punisce chiunque, avendo commesso o concorso a commettere un delitto non colposo, impieghi, sostituisca, trasferisca, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto in modo da ostacolare concretamente l'identificazione della provenienza delittuosa.

11.11.1 Le attività sensibili ai fini del D.Lgs. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica tra gli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui all'art. 25^{octies} del Decreto, le seguenti **attività sensibili** della Società:

- Selezione e gestione dei fornitori;
- Gestione della clientela;
- Selezione e gestione dei consulenti;

- Gestione dei flussi finanziari;
- Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.12 I delitti in materia di violazione del diritto d'autore – art. 25^{novies}, D.Lgs. n. 231/01

Con riferimento all'art. 25^{novies} del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Art. 17,1 comma 1, lett a - bis) e comma 3, L. n. 633/1941

La norma sanziona la condotta di chi, senza averne diritto, a qualsiasi scopo e in qualsiasi forma mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa. La fattispecie è aggravata se il reato è commesso sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Art. 171bis, L. n. 633/1941

La norma riconosce la penale responsabilità di chi, 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). La stessa pena si applica 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. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità oppure chi, 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 di dati in violazione delle disposizioni di cui agli artt. 64^{quinquies} e 64^{sexies}, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli artt. 102^{bis} e 102^{ter}, ovvero distribuisce, vende o concede in locazione una banca di dati.

Art. 171ter, L. n. 633/1941

La norma sanziona chi 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; 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; 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 lettere a) e b); 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, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; 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; 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; 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 tecnologiche di cui all'art. 102^{quater} 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; abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102^{quinquies}, 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 stesse; riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1; promuove o organizza le attività illecite di cui al comma 1.

Art. 171^{septies}, L. n. 633/1941

Sanziona chi dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'art. 181^{bis}, comma 2, della legge sul diritto d'autore nonché i produttori o importatori dei supporti non soggetti al contrassegno di cui all'art. 181^{bis} della stessa legge, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi.

Art. 171octies, L. n. 633/1941

La norma punisce chi, a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato 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. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

11.12.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, tra gli elementi essenziali del Modello di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati in materia di violazione del diritto d'autore, le seguenti **attività sensibili** della Società:

- Utilizzo di strumenti informatici (pc) da Utenti;
- Utilizzo di strumenti informatici (pc) da Amministratori di sistema;
- Utilizzo di opere di ingegno coperte dal diritto d'autore.

Per ogni attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità del singolo soggetto interessato segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.13 I delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria – art. 25decies, D.Lgs. n. 231/01

Con riferimento all'art. 25decies del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

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

La norma sanziona l'ipotesi di chi, salvo che il fatto non costituisca reato più grave, con violenza o minaccia o con offerta o promessa di denaro o di altra utilità, induce la persona chiamata a rendere dichiarazioni utilizzabili in un procedimento penale a non rendere dichiarazioni o a rendere dichiarazioni mendaci, quando questa ha la facoltà di non rispondere.

11.13.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali del Modello di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui all'art. 25^{decies} del Decreto, le seguenti **attività sensibili** della Società:

- Rapporti con l'Autorità giudiziaria nell'ambito di procedimenti penali.

Per tale attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **oggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.14 I reati ambientali – art. 25^{undecies}, D.Lgs. n. 231/01

Con riferimento all'art. 25^{undecies} del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nelle seguenti fattispecie criminose (consumate o tentate):

Attività di gestione di rifiuti non autorizzata (art. 256, comma 1, lett. a) e b), D.lgs. n. 152/06).

La norma punisce chiunque, fuori dai casi sanzionati ai sensi dell'art. 29^{quattordices}, comma 1, effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli artt. 208 - 209 - 210 - 211 - 212 - 214 - 215 - 216.

Predisposizione ed uso di un falso certificato di analisi dei rifiuti (art. 258 comma 4 e art. 260^{bis}, commi 6 e 7, D.lgs. n. 152/06)

Traffico illecito di rifiuti (art. 259, comma 1, D.lgs. n. 152/06)

La norma punisce chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'art. 26 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'art. 1, comma 3, lettere a), b), c) e d), del regolamento stesso. La pena è aumentata in caso di spedizione di rifiuti pericolosi.

Attività organizzate per il traffico illecito di rifiuti (art. 260, D.lgs. n. 152/06)

La norma 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.

Se si tratta di rifiuti ad alta radioattività si applica la pena è aumentata.

Violazioni del sistema di controllo sulla tracciabilità dei rifiuti (art. 260bis, comma 8, D.lgs. n. 152/06)

11.14.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati ambientali, la seguente **attività sensibile** della Società:

- Gestione dei prodotti e rifiuti, compilazione dei registri di controllo e flussi informativi verso le Autorità di Vigilanza.

Per tale attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

Nell'ambito dell'attività evidenziate, la Società si impegna a predisporre un efficace sistema di gestione ambientale che punti a realizzare la politica ambientale dell'organizzazione ed a conseguire gli obiettivi di miglioramento definiti dal vertice aziendale. Il sistema deve specificare responsabilità, mezzi, procedure operative, esigenze di formazione, provvedimenti di monitoraggio e controllo, sistemi di comunicazione.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

11.15 I reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare – art. 25duodecies, D.Lgs. n. 231/01

Con riferimento all'art. 25duodecies del Decreto, i reati presupposto della responsabilità amministrativa TIP possono essere identificati nella seguente fattispecie criminosa (consumata o tentata):

Art. 22, comma 12bis, Lavoro subordinato a tempo determinato e indeterminato, D.lgs. n. 286/1998, Testo unico sull'immigrazione

La norma punisce il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato.

La pena è aggravata:

- a) se i lavoratori occupati sono in numero superiore a tre;
- b) se i lavoratori occupati sono minori in età non lavorativa;
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'art. 603bis c.p.

11.15.1 Le attività sensibili ai fini del D.Lgs. n. 231/01

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali del Modello di organizzazione, gestione e controllo, l'individuazione delle cd. attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati ex art. 25*duodecies*, la seguente **attività sensibile** della Società:

- Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale.

Per tale attività sensibile è stato predisposto un **protocollo operativo** corrispondente (allegato al Modello) nel quale sono indicati i **soggetti responsabili** e gli **strumenti di prevenzione, controllo e contrasto** dei reati presupposto della responsabilità ex D.lgs. n. 231/01.

E' responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche o integrazioni da apportare alla presente Parte Speciale.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) dei protocolli operativi;
- b) dei principi di comportamento individuati nel Codice Etico;
- c) di quanto regolamentato dalla documentazione organizzativa interna;
- d) delle disposizioni di legge.

12. PROTOCOLLI OPERATIVI

12.1 Gestione dei contenziosi giudiziari e stragiudiziali (es. accordi transattivi, contenzioso giuslavoristico, contenzioso tributario)

- ✓ **Potere decisionale:** Presidente e Amministratore Delegato o Consiglio di Amministrazione
- ✓ **Potere di gestione:** Avvocato con il supporto del soggetto coinvolto
- ✓ **Potere di controllo:** Internal Audit (anche per il tramite di uno dei suoi componenti)

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei contenziosi giudiziari e stragiudiziali di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)
- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 319^{ter} c.p., Corruzione in atti giudiziari
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
- ❖ i reati societari, previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2635^{bis} c.c., Istigazione alla corruzione tra privati
- ❖ i reati in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, previsti dall'art. 25^{decies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 377^{bis} c.p., Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Regolamentazione: obiettivo delle procedure e dei controlli di seguito specificati è di assicurare la correttezza, la trasparenza e la tracciabilità dei rapporti sia con l'Autorità Giudiziaria sia verso i terzi, anche quando sono gestiti per il tramite di un legale esterno. A seconda delle tipologie di procedimento, vengono riportate le principali fasi del processo.

Ci si riporta, nell'ambito dei poteri decisionali, alle procure e deleghe in essere *ad hoc* per i procedimenti giudiziari e stragiudiziali.

Nell'ambito di tale processo, definiti ruoli e responsabilità dei soggetti incaricati di gestire le differenti fasi, sono previsti i protocolli di prevenzione che da questi devono essere applicati.

Nel caso di contenzioni tributari, è sempre informato l'*Internal Audit* per fornire il proprio parere, non vincolante.

In particolare, è prevista:

- Attivazione del contenzioso, previa informativa, da parte del Presidente e, se diverso, del Soggetto Coinvolto;
- Nomina del legale esterno e gestione operativa del contenzioso con l'ausilio del Responsabile di Area competente e del Amministratore Delegato e, se diverso, del Soggetto Coinvolto;
- Verifica della prestazione e controllo del rispetto delle procedure da parte dell'*Internal Audit*. L'attivazione di qualsivoglia procedimento e il suo esito devono essere comunicate con nota operativa dall'Amministratore Delegato all'Organismo di Vigilanza. Si precisa che nessun tipo di dazione in denaro o altra utilità è autorizzata nei confronti di soggetti giudicanti (giudice, arbitro, mediatore, ecc.) al fine di influenzare il giudizio.

1. La fase di attivazione del contenzioso vede alcune differenze, nel caso di procedimento attivo o passivo:

- a. Per i contenziosi attivi, dopo aver ricevuto l'informativa, il Presidente dà mandato all'Amministratore Delegato di raccogliere tutta la documentazione che ritiene utile in merito; il Presidente con l'Amministratore Delegato decide se promuovere il contenzioso;
- b. Per i contenziosi passivi, ricevuta l'informativa, l'Amministratore Delegato raccoglie tutta la documentazione necessaria. Il Presidente valuta come procedere. Il Presidente nomina, sentito l'Amministratore Delegato, il legale esterno e decidono se procedere in via stragiudiziale, se possibile, ovvero concertano la strategia processuale. Inoltre, informano il Consiglio di Amministrazione.

2. Nell'ambito della gestione del contenzioso, l'Amministratore Delegato cura i rapporti con il legale esterno per presidiare le seguenti attività:

- Valutazione della possibilità di addivenire ad una transazione;
- Gestione dell'istruttoria della causa attraverso la raccolta della documentazione e delle informazioni utili alla stesura del promemoria da trasmettere al legale esterno per la preparazione degli atti iniziali e di quelli successivi;
- Analisi degli atti predisposti dal legale esterno al fine di proporre eventuali modifiche e integrazioni;
- Verifica e valutazione degli atti di causa;
- Informazione costante al Presidente e, se diverso, al Soggetto Coinvolto nonché al Consiglio di Amministrazione anche per il tramite di uno dei suoi componenti circa l'andamento della causa;
- Comunicazione al Presidente e, se diverso, al Soggetto Coinvolto nonché al Consiglio di Amministrazione, anche per il tramite di uno dei suoi componenti della chiusura del contenzioso e dell'esito dello stesso.

Nel caso di accordi transattivi, una volta definito l'accordo, il legale esterno, con il costante ausilio dell'Amministratore Delegato, presenta bozza dell'accordo transattivo al Presidente, che approva. Si precisa che la documentazione prodotta non può subire alcuna alterazione; deve pertanto esserne garantita l'integrità e la veridicità.

3. L'*internal audit*, anche per il tramite di uno dei suoi componenti, cura la correttezza della prestazione e delle procedure. In caso di violazioni o pericoli di commissione di reati, informa l'Organismo di Vigilanza.

Documenti di riferimento:

- Regolamento disciplinare aziendale per le controversie giuslavoristiche
- Procedura - Selezione e assunzione del personale
- Procedura - Spese
- Codice Etico dipendenti e collaboratori

Tracciabilità: tutte le fasi del processo di attivazione, gestione e verifica del contenzioso sono opportunamente documentate e comunicate tra soggetti coinvolti, anche via mail, per l'archiviazione della relativa documentazione. L'Amministratore Delegato cura l'archiviazione della documentazione, che deve avvenire in armadio chiuso dotato di serratura ovvero, se su supporto telematico, attraverso un accesso chiuso. Le chiavi e gli identificativi sono a disposizione del Presidente e dell'Amministratore Delegato.

12.2 Rapporti con l'Autorità Giudiziaria nell'ambito di procedimenti penali

- ✓ **Potere decisionale: Presidente e Amministratore Delegato o Consiglio di Amministrazione**
- ✓ **Potere di gestione: Avvocato penalista esterno e Soggetto coinvolto**
- ✓ **Potere di controllo: Organismo di Vigilanza**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei rapporti tra TIP e l'Autorità Giudiziaria nell'ambito di procedimenti penali che coinvolgono la Società, i suoi soggetti apicali o sottoposti al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)
- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 319^{ter} c.p., Corruzione in atti giudiziari
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
- ❖ i reati in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, previsti dall'art. 25^{decies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 377^{bis} c.p., Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Regolamentazione: la presente area sensibile non presuppone una vera e propria distinzione per fasi. Quando viene aperto un procedimento penale nei confronti della Società ciascun destinatario del

Modello chiamato a svolgere un ruolo attivo rispetto alle richieste dell'Autorità Giudiziaria (il "Destinatario") deve preliminarmente informare l'Amministratore Delegato, se non direttamente coinvolto, ovvero, in tale ipotesi, l'intero Consiglio di Amministrazione, che si impegna a garantire la serenità e la collaborazione necessaria al rispetto delle richieste avanzate. Qualora necessario, il Destinatario chiede il supporto di competenze esterne.

Il Destinatario è tenuto al rispetto dei seguenti principi:

- a. Rispetto dei criteri di trasparenza e verità;
- b. Totale disponibilità e collaborazione rispetto alle richieste dell'Autorità Giudiziaria;
- c. Accesso a tutte le informazioni societarie necessarie per rispondere alle richieste dell'Autorità Giudiziaria;
- d. Assistenza giudiziale, in caso di necessità, qualora il procedimento penale sia connesso alle attività svolte dal destinatario per la Società e queste ne abbiano determinato il coinvolgimento.

Qualora qualsiasi Soggetto coinvolto subisca pressioni, siano esse realizzate con condotte violente o minatorie oppure per il tramite di corresponsione di somme di denaro o di qualsivoglia vantaggio, atte a inibire la completa collaborazione alle richieste dell'Autorità giudiziaria ovvero a dissimulare la realtà dei fatti, è tenuto immediatamente per iscritto a informare l'Organismo di Vigilanza, astenendosi dalla condotta in violazione delle prescrizioni indicate dal presente Modello.

Documenti di riferimento:

- Codice Etico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. In particolare, ogni richiesta alla Pubblica Amministrazione e ogni processo decisionale prevede apposita verbalizzazione, in assenza di altra evidenza documentale, da parte dell'Amministratore Delegato. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali.

12.3 Gestione dei rapporti con l'Amministrazione Finanziaria (es. predisposizione della dichiarazione dei redditi o dei sostituti di imposta)

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: CFO e Consulente esterno**
- ✓ **Potere di controllo: Presidente e Dirigente Preposto**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei rapporti tra TIP e l'Amministrazione Finanziaria al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di indebita percezione di erogazioni, truffa ai danni dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico, previsti dall'art. 24 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 640 c.p., Truffa

- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso

- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{bis} c.p., Circostanze aggravanti
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

Regolamentazione: il processo in oggetto si suddivide nelle seguenti macrofasi:

1. Raccolta della documentazione necessaria;
2. Predisposizione delle dichiarazioni;
3. Autorizzazione delle dichiarazioni;
4. Presentazione delle dichiarazioni;
5. Verifiche.

Il Modello garantisce il corretto flusso di tutte le informazioni e documenti utili e necessari ad assolvere gli obblighi di cui al presente paragrafo da parte della Società.

1. La fase di raccolta della documentazione è predisposta, con la collaborazione, se del caso, del consulente esterno, che ottiene tutta la documentazione necessaria alla predisposizione delle dichiarazioni fiscali e alla liquidazione dei relativi tributi;
2. La fase di predisposizione delle dichiarazioni, svolta dal consulente esterno di concerto col CFO, prevede la raccolta dei dati e delle informazioni, la cui correttezza, veridicità e genuinità è verificata scrupolosamente prima dell'invio delle stesse. La Società richiede al consulente esterno di segnalare i casi di dubbia interpretazione di norme tributarie che possano generare un risparmio di imposta al fine di garantirne la correttezza e di non determinare forme di evasione fiscale.
3. La fase di autorizzazione delle dichiarazioni è avallata dall'Amministratore Delegato, che le valuta, alla luce della documentazione raccolta e dei contenuti della stessa. Congiuntamente è svolto un controllo da parte della Società di Revisione, che certifica il bilancio e sottoscrive le conseguenti dichiarazioni fiscali, del Collegio Sindacale e dell'Amministratore Delegato;
4. La fase di presentazione delle dichiarazioni è subordinata al consenso dell'Amministratore Delegato o del Dirigente Preposto ed è svolta dal CFO;
5. Il Collegio Sindacale, il Presidente, l'Amministratore Delegato e il Dirigente Preposto svolgono i controlli sulla correttezza delle procedure, sulla veridicità delle attestazioni contenute nelle

dichiarazioni e sulla rispondenza delle stesse con la normativa di riferimento. In caso ravvisino violazioni nelle procedure o aree di rischio di reato, informano l'Organismo di Vigilanza.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. In particolare, ogni richiesta alla Pubblica Amministrazione e ogni processo decisionale prevede apposita verbalizzazione, in assenza di altra evidenza documentale, da parte del CFO. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo al medesimo Amministratore Delegato.

12.4 Gestione degli adempimenti e delle comunicazioni con le Autorità pubbliche di vigilanza

- ✓ **Potere decisionale: Presidente, Amministratore Delegato**
- ✓ **Potere di gestione: Amministratore Delegato e Assistente alla Direzione**
- ✓ **Potere di controllo: Consiglio di Amministrazione**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione degli adempimenti e della comunicazione tra TIP e le Autorità pubbliche di vigilanza al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ **i reati in materia di criminalità organizzata**, previsti dall'art. 24ter del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416bis c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416ter c.p., Scambio elettorale politico-mafioso
- ❖ **i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione**, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319bis c.p., Circostanze aggravanti
 - Art. 319quater c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 322bis c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

- ❖ i reati societari, previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2638 c.c., Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

Regolamentazione: il processo in oggetto è regolamentato da apposita documentazione organizzativa interna che disciplina le attività di gestione degli adempimenti e dei rapporti con le Autorità pubbliche.

Il processo si suddivide nelle seguenti macrofasi:

1. Monitoraggio delle scadenze e delle disposizioni normative o richieste di chiarimento;
2. Analisi della richiesta e dell'adempimento ed attivazione dei soggetti competenti;
3. Analisi della completezza della documentazione da trasmettere;
4. Resoconti periodici;
5. Verifiche.

Nell'ambito di tale processo, vengono di seguito definiti ruoli e responsabilità dei soggetti incaricati di gestire le differenti fasi, nonché i protocolli di prevenzione che da questi devono essere applicati. In particolare:

1. La fase di monitoraggio delle scadenze di disposizioni normative o richieste di chiarimento prevede che l'Amministratore Delegato, anche avvalendosi di consulenti esterni e personale interno, monitori l'insorgere di eventuali richieste di chiarimenti o informazioni formulate dalle Autorità Pubbliche.
2. La fase di analisi della richiesta dell'adempimento ed attivazione dei soggetti competenti prevede che l'Amministratore Delegato si attivi per la predisposizione e raccolta della documentazione richiesta dall'Autorità o per il relativo adempimento. L'Amministratore Delegato si avvale dell'Assistente alla Direzione e, se del caso, dell'ausilio di consulenti esterni. L'Amministratore Delegato controlla inoltre la documentazione predisposta, assicurandone la correttezza, la veridicità e l'aggiornamento.
3. La fase di analisi della completezza della documentazione da trasmettere prevede che l'Amministratore Delegato, prima della trasmissione all'Autorità referente, effettui una verifica della documentazione fornita.
4. L'Amministratore Delegato aggiorna regolarmente il Consiglio di Amministrazione. Il Consiglio di Amministrazione verifica che tutte le procedure indicate siano correttamente seguite. Qualora non siano chiari alcuni processi il Consiglio di Amministrazione chiede informazioni all'Amministratore Delegato, che fornisce le indicazioni richieste. In caso di violazioni o possibili rischi di reato, il Consiglio di Amministrazione informa l'Organismo di Vigilanza.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: le principali fasi del processo devono essere opportunamente documentate e archiviate presso gli uffici dell'Amministratore Delegato.

In particolare:

- Devono essere tracciate ed archiviate presso l'Amministratore Delegato tutte le richieste di documentazione, i chiarimenti e le informazioni formulati dalle Autorità Pubbliche di Vigilanza.

- Deve essere tracciato ed archiviato, ad opera dell'Amministratore Delegato eventualmente, quale mero supporto operativo, con l'Assistente alla Direzione, tutto il processo interno che ha condotto ad elaborare il documento e ad autorizzarne la trasmissione all'esterno, con particolare riferimento ai controlli intermedi eseguiti.

In caso di assenza di evidenza documentale, è predisposta verbalizzazione di quanto accaduto dall'Amministratore Delegato e sottoposta all'approvazione dal Consiglio di Amministrazione.

12.5 Gestione dei rapporti, anche in caso di ispezioni, con soggetti pubblicisticamente qualificati, con Autorità di Vigilanza e controllo in materia fiscale, tributaria, societaria e finanziaria, ambientale, previdenziale, sanitaria, di sicurezza e igiene sul lavoro, prevenzione degli infortuni sul lavoro e assistenziale in genere, di immigrazione, espatrio da parte di personale proveniente da paesi extracomunitari

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Amministratore Delegato e i Preposti dell'Area di Riferimento**
- ✓ **Potere di controllo: Consiglio di Amministrazione**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei rapporti di TIP con soggetti pubblicisticamente qualificati e con Autorità di Vigilanza e controllo, anche in caso di ispezioni, al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di indebita percezione di erogazioni, truffa ai danni dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico, previsti dall'art. 24 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 640 c.p., Truffa
- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{bis} c.p., Circostanze aggravanti
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio

- Art. 322*bis* c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

Regolamentazione: Il processo in esame si suddivide in macrofasi:

1. Informativa dell'insorgere del rapporto con soggetti pubblicisticamente qualificati o con Autorità di vigilanza e controllo;
2. Gestione del rapporto;
3. Esito ed eventuale gestione degli adempimenti derivanti o delle sanzioni eventualmente applicate;
4. Verifiche.

1. Qualora la Società intrattenga rapporti a fini ispettivi con soggetti pubblicisticamente qualificati, con Autorità di Vigilanza e controllo, colui che ne viene a conoscenza informa tempestivamente l'Amministratore Delegato ovvero, in materia di D.lgs. n. 81/2008, il Datore di Lavoro.

2. Nella gestione del rapporto, il Preposto all'Area di riferimento fornisce tutte le informazioni e la documentazione richiesta dai soggetti indicati in oggetto, assistendo l'Amministratore Delegato ovvero, in materia di D.lgs. n. 81/2008, il Datore di Lavoro, che gestisce il rapporto con l'Autorità di Vigilanza in prima persona. Il Preposto all'Area di riferimento dà informativa di ogni chiarimento o richiesta da parte dei soggetti pubblicisticamente qualificati a coloro che sono indicati in ordine al potere decisionale, secondo le rispettive competenze.

3. Il Preposto all'Area di riferimento attende l'esito dell'accesso dei soggetti pubblicisticamente qualificati e informa coloro che esercitano il potere decisionale, secondo le rispettive competenze. L'Amministratore Delegato, in caso di sanzioni, conferisce incarico di pagamento. L'Amministratore Delegato e/o il Preposto all'Area di riferimento dà inoltre indicazioni al fine di addivenire a tutte le migliorie o integrazioni procedurali per adeguarsi alle normative ed evitare ulteriori sanzioni. In caso di problematiche di sorta, il Preposto all'Area di riferimento sottopone la questione all'Amministratore Delegato ovvero, in materia di D.lgs. n. 81/2008, al Datore di Lavoro, che, secondo le proprie competenze, effettuano le valutazioni del caso e decidono come procedere, informando il Consiglio di Amministrazione, anche per il tramite di un suo componente.

4. Il Datore di Lavoro o l'Amministratore Delegato, a seconda dei casi, svolge i controlli sulla correttezza delle procedure, sulle violazioni di legge eventuali e, in caso di sanzioni, sull'attività di adeguamento alle previsioni di legge. In caso egli ravvisi violazioni nelle procedure o aree di rischio di reato o comunque violazioni di legge, informa l'Organismo di Vigilanza ovvero, in materia di D.lgs. n. 81/2008, il RSPP.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Procedura per l'affidamento di lavori in appalto

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura del Datore di Lavoro o Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante

credenziali note solo all'Amministratore Delegato ovvero, in materia di D.lgs. n. 81/2008, al Datore di Lavoro.

12.6 Richiesta, ottenimento e gestione dei rapporti con soggetti pubblicisticamente qualificati in occasione del conseguimento o rinnovo di abilitazioni, concessioni, autorizzazioni, certificazioni e licenze, comunque denominate, rilasciate per l'esercizio dell'attività d'impresa

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Responsabile competente e Assistente alla Direzione (si occupa solo delle formalità compilatorie e dell'invio delle comunicazioni con Borsa Italiana e Consob)**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei rapporti di TIP con soggetti pubblicisticamente qualificati in occasione del conseguimento o del rinnovo di abilitazioni, concessioni, autorizzazioni certificazioni e licenze per l'esercizio dell'attività di impresa al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di indebita percezione di erogazioni, truffa ai danni dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico, previsti dall'art. 24 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 640 c.p., Truffa
- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{bis} c.p., Circostanze aggravanti
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

Regolamentazione: il processo in esame si suddivide in macrofasi:

1. Verifica della necessità di richiesta o rinnovo dell'abilitazione, concessione, autorizzazione, certificazione o licenza;
2. Analisi ed eventuale integrazione della documentazione e predisposizione degli adempimenti necessari;
3. Formalizzazione della richiesta o del rinnovo;
4. Monitoraggio dell'iter autorizzativo ed esito;
5. Verifiche.

1. L'Amministratore Delegato verifica regolarmente per il tramite di suoi incaricati la necessità di ottenere o rinnovare abilitazioni, concessioni, autorizzazioni, certificazioni, licenze ed esprime parere sull'esistenza dei requisiti e sull'opportunità.

2. L'Assistente alla Direzione, o coloro incaricati dall'Amministratore Delegato, chiedono la documentazione al personale competente. La Società può avvalersi anche dell'eventuale ausilio di consulenti esterni.

3. L'Assistente alla Direzione, sulla base delle indicazioni ricevute, avanza la richiesta, verificando con attenzione e prudenza la veridicità della documentazione e delle dichiarazioni prodotte;

4. L'Assistente alla Direzione monitora l'iter autorizzativo della richiesta; non appena ne viene a conoscenza, informa l'Amministratore Delegato dell'esito. Acquisisce l'abilitazione, la concessione, l'autorizzazione, la certificazione o la licenza. In caso di difformità o problematiche di sorta, il Responsabile di Area competente effettua le valutazioni del caso, informandone l'Amministratore Delegato.

5. Il Presidente svolge i controlli sulla correttezza delle procedure. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, informa l'Organismo di Vigilanza.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Documenti allegati alla Procedura per l'affidamento di lavori in appalto in riferimento al D. Lgs. 81/08

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo all'Amministratore Delegato e al Presidente.

12.7 Gestione dei flussi finanziari

- ✓ **Potere decisionale:** Amministratore Delegato o Presidente
- ✓ **Potere di gestione:** Ufficio di Segreteria
- ✓ **Potere di controllo:** CFO

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei flussi finanziari di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di abusi di mercato, previsti dall'art. 25^{sexies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
 - Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
- ❖ i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, previsti dall'art. 25^{octies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 648 c.p., Ricettazione
 - Art. 648^{bis} c.p., Riciclaggio
 - Art. 648^{ter} c.p., Impiego di denaro, beni o utilità di provenienza illecita
 - Art. 648^{ter.1} c.p., Autoriciclaggio

Regolamentazione: il processo oggetto è regolamentato da apposita documentazione organizzativa, che disciplina la gestione dei flussi finanziari. Si suddivide in macrofasi:

1. Informativa dei flussi finanziari in uscita e in entrata;
2. Controlli in merito ai flussi finanziari;
3. Verifiche.

1. L'Amministratore Delegato, previa richiesta e/o presentazione di relativi giustificativi viene informato dei flussi in uscita e in entrata imputandoli a soggetti specifici. L'Amministratore Delegato dà eventuale approvazione ad effettuare pagamenti e/o, ricevere flussi in entrata. Con riferimento ai flussi in uscita, il processo deve essere strutturato con l'obiettivo di assicurare che tutte le uscite finanziarie siano opportunamente giustificate e documentate, effettuate secondo le specifiche responsabilità e i controlli nonché nel rispetto delle previsioni del presente Modello.

2. Qualora i dati sui flussi finanziari siano qualificabili come informazioni privilegiate (anche in base alla mappatura effettuata in merito alla tipologia di informazioni rilevanti), trova applicazione quanto previsto dalle procedure interne in materia di iscrizione nell'Insider List. Pertanto, qualora l'Ufficio di Segreteria non sia stato classificato come una FOCIP (funzione organizzativa competente informazioni privilegiate) in relazione al caso di specie, l'Amministratore Delegato coinvolge soltanto i soli addetti che siano già iscritti nell'Insider List. Qualora sia necessario il coinvolgimento di altri addetti non iscritti, provvede a richiedere preventivamente l'iscrizione del/degli addetti coinvolto/i nell'Insider List ex art. 115-bis TUF. L'Amministratore Delegato ed il Presidente hanno la firma sul conto in banca e l'Assistente all'Ufficio di Segreteria ha una delega ai prelievi/versamenti. Il pagamento di fornitori deve avvenire sul conto corrente intestato a tale soggetto e in nessun modo può avvenire su conti correnti cifrati, nei confronti di soggetti diversi dai destinatari e su conti correnti di banche appartenenti a paradisi fiscali o società *off shore*, salvo che vi sia specifica legittimità e congruenza di tali pagamenti. Quanto ai flussi in entrata, il CFO verifica la corretta esecuzione, la provenienza degli stessi da chi è legittimato (controparte contrattuale) e non da soggetti non identificabili ovvero in assenza di apposito

giustificativo o ancora in un paese differente da quello dei contraenti o di esecuzione del contratto, salvo che ci sia apposita giustificazione circa la legittimità e la congruenza di tali pagamenti. Il CFO, su indicazione o richiesta dell'Amministratore Delegato o del Presidente dà l'assenso a solleciti ovvero a richieste finanziarie in virtù delle decisioni aziendali.

3. Il CFO verifica la corretta imputazione e la coerenza con i limiti di spesa, anche in relazione alle deleghe e alle procure aziendali, ovvero con i preventivi stabiliti. Dietro apposito giustificativo, fornito su richiesta dei Responsabili di Area nonché di esigenze contabili, l'Amministratore Delegato delibera i flussi in uscita, anche nel rispetto delle previsioni di spesa. Qualora riscontrasse problematiche o difformità chiede informazioni ai Responsabili di Area competenti, dandone informativa al CFO.

4. Il CFO verifica la correttezza e l'adeguata motivazione dei flussi in uscita e in entrata, svolge i controlli sulla correttezza delle procedure, sulla rispondenza del rapporto contrattuale con le esigenze evidenziate e sull'esecuzione delle previsioni contrattuali. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, informa l'Organismo di Vigilanza.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Procedura gestione registro dei soggetti aventi accesso alle informazioni privilegiate
- Procedura di gestione del registro dei soggetti aventi accesso alle informazioni privilegiate

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo allo stesso.

12.8 Predisposizione di bilanci, relazioni e comunicazioni sociali in genere

- ✓ **Potere decisionale: Consiglio di Amministrazione**
- ✓ **Potere di gestione: Presidente, Amministratore Delegato, Dirigente preposto, CFO con il supporto di un consulente esterno**
- ✓ **Potere di controllo: Collegio Sindacale e Revisore Contabile**
- ✓ **Potere di controllo su informazioni privilegiate: Amministratore Delegato e Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di predisposizione dei bilanci, delle relazioni e delle altre comunicazioni sociali di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ **i reati societari,** previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2621 c.c., False comunicazioni sociali
 - Art. 2621^{bis} c.c., Fatti di lieve entità
 - Art. 2622 c.c., False comunicazioni sociali delle società quotate

- Art. 2624 c.c., Falsità nelle relazioni o nelle comunicazioni delle società di revisione
 - Art. 2625 c.c., Impedito controllo
 - Art. 2626 c.c., Indebita restituzione dei conferimenti
 - Art. 2627 c.c., Illegale ripartizione degli utili e delle riserve
 - Art. 2628 c.c., Illecite operazioni sulle azioni o quote sociali o della società controllante
 - Art. 2629 c.c., Operazioni in pregiudizio dei creditori
 - Art. 2632 c.c., Formazione fittizia del capitale
 - Art. 2638 c.c., Ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza
 - Art. 2635 c.c., Corruzione tra privati
 - Art. 2635*bis* c.c., Istigazione alla corruzione tra privati
- ❖ i reati in materia di abusi di mercato, previsti dall’art. 25*sexies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
- Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
 - Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria

Regolamentazione: il processo in oggetto è regolamentato da apposita documentazione organizzativa interna e da procedure amministrativo-contabili introdotte a seguito delle attività svolte dalla Società per ottemperare alla normativa di riferimento.

Il processo di predisposizione del progetto di bilancio e dei documenti collegati viene distinto nelle seguenti macrofasi:

1. Gestione della contabilità generale;
2. Valutazione e stima delle poste in bilancio;
3. Predisposizione del bilancio civilistico.

È prevista la possibilità di avvalersi di consulenti esterni in ogni fase.

1. Nell’ambito del processo devono essere definiti ruoli, responsabilità ed attività di controllo, in particolare, con riferimento alle diverse fasi del processo:

La fase di gestione della contabilità generale e del contenuto del piano dei conti di contabilità generale viene assegnata al CFO. Le scritture e le registrazioni contabili vengono effettuate in modo da riflettere accuratamente e correttamente tutte le operazioni della Società. La società si avvale a questo fine di una struttura esterna. Eventuali modifiche ai criteri di contabilizzazione proposti sono verificate dal CFO, dal Dirigente Preposto e dalla Società di Revisione.

Tutte le poste di carattere economico e patrimoniale sono rappresentate in contabilità in modo veritiero, corretto e opportunamente documentate in conformità alla legislazione vigente. La rilevazione delle informazioni contabili avviene tramite sistema informatico, a garanzia della tracciabilità dei singoli passaggi del processo di formazione dei dati. Sono previste credenziali di accesso che consentano l’identificazione dell’autore della comunicazione. Sono garantite la separazione delle funzioni e la coerenza dei livelli autorizzativi. Qualora siano formulate ingiustificate/anomale richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile (da chiunque provenienti), di variazione quantitative dei dati rispetto a quelli già contabilizzati in base alle procedure correnti, chi ne è

a conoscenza informa per iscritto il Collegio Sindacale. La fase di valutazione e stima delle poste di bilancio si articola nelle seguenti attività:

- Predisposizione delle ipotesi di stima e valutazione da parte del CFO. Tali valutazioni e stime sono controllate da Presidente, Amministratore Delegato e Dirigente Preposto;
- Verifica delle metodologie di rappresentazione contabile delle poste valutative e del loro andamento da parte della Società di Revisione.

2. La fase di predisposizione del bilancio civilistico può essere suddivisa in:

- Predisposizione e diffusione del calendario finanziario: l'Amministratore Delegato, sentito il Consiglio di Amministrazione, redige un calendario finanziario che riporta le date delle riunioni del Consiglio di Amministrazione chiamato ad approvare le diverse situazioni di chiusura trimestrali, semestrali ed annuali nonché la relativa assemblea dei soci e pubblica sul sito della Società tali date;
- Gestione delle attività di chiusura del bilancio: il CFO con l'ausilio del consulente esterno provvede ad effettuare le registrazioni in contabilità generale per il periodo in chiusura e provvede ad ottenere da tutte le aree coinvolte nel processo di predisposizione del bilancio d'esercizio i dati contabili di chiusura;
- Predisposizione del progetto di bilancio: il CFO redige gli schemi contabili e la nota integrativa il Presidente, il Vice Presidente esecutivo e il Dirigente Preposto redigono la Relazione illustrativa sull'andamento della Gestione.

Il Dirigente Preposto controlla tutte le scritture contabili e l'appostazione di tutte le poste di bilancio secondo le procedure definite dall'autorità competente;

- Prima della seduta del Consiglio di Amministrazione indetta per l'approvazione del bilancio di esercizio si tiene la riunione tra tutti gli Organismi di Controllo compreso il Comitato Controllo e Rischi e Parti Correlate per le parti ad esso relative;
- Approvazione del progetto di bilancio: il progetto di bilancio viene portato all'attenzione del Consiglio di Amministrazione.
- Dopo l'approvazione da parte del Consiglio di Amministrazione la società di revisione ha 15 giorni per effettuare i controlli relativi al bilancio approvato dal Consiglio di Amministrazione. La bozza di bilancio e gli altri documenti contabili devono essere messi a disposizione degli amministratori e del Revisore con ragionevole anticipo. Il Consiglio di Amministrazione approva il bilancio, che invia al Collegio Sindacale nei termini di legge. Analogamente sia il Revisore, per la sua parte di competenza, che il Collegio Sindacale redigono le relative relazioni.
- Alla conclusione delle proprie attività, la Società di Revisione presenta in un incontro con l'Amministratore delegato, il Dirigente Preposto il Collegio Sindacale e i rappresentanti del comitato controllo e rischi i risultati dell'attività di audit, ma non rende noto il testo della relazione di revisione, né il giudizio finale. Trovano applicazione le procedure interne in relazione alla valutazione di quanto rappresentato dalla società di revisione nell'incontro. Qualora ad esito della riunione un'informazione costituisca informazione privilegiata, l'Amministratore Delegato ed il Presidente valutano se: pubblicarla o, in alternativa, qualora ne sussistano le condizioni, ritardarne la pubblicazione.
- Successivamente, il Revisore trasmette la Relazione di revisione contenente il giudizio finale. L'Amministratore Delegato e il Presidente valutano se la stessa costituisca un'informazione privilegiata. Qualora la Relazione di revisione sia ritenuta un'informazione privilegiata, l'Amministratore Delegato provvede alla pubblicazione ai sensi della disciplina in materia di comunicazione di informazioni privilegiate.

- Tutte le relazioni presenti e i giudizi sul bilancio sono messi a disposizione del Consiglio di Amministrazione e del Collegio Sindacale prima che venga indetta l'Assemblea dei soci per l'approvazione;
- Approvazione del Bilancio d'esercizio: il Progetto di Bilancio d'esercizio, corredato delle Relazioni previste per legge, viene sottoposto all'approvazione dell'Assemblea dei Soci per la delibera.

Ulteriori disposizioni in materia di prevenzione dei reati di cui agli art. 184 e 185 TUF

Poiché il processo di redazione del Progetto di Bilancio di esercizio (anche in base alla mappatura dei tipi di informazioni rilevanti), può generare informazioni privilegiate ex art. 181 TUF:

- a. trova applicazione quanto previsto dalle procedure interne in materia di attivazione dell'Insider List;
 - i. l'Amministratore Delegato verifica che nella gestione del processo di redazione del Progetto di Bilancio – fino alla sua pubblicazione - siano rispettate le misure di sicurezza organizzativa, fisica e logica delle specifiche informazioni rilevanti (es. controllare l'accesso alle specifiche informazioni rilevanti, la strutturazione su diversi livelli di accesso, la protezione dei relativi supporti informatici tramite parole chiave, crittografia, ecc.) ed impone limiti alla circolazione di dati e documenti *ad hoc*, se ritenuto necessario);
 - ii. verifica che gli uffici coinvolti siano classificati come FOCIP (funzione organizzativa competente informazioni privilegiate). Il CFO non può coinvolgere soggetti – interni o esterni a TIP – che non siano stati preventivamente iscritti nell'Insider List – ovvero opera in modo tale tali addetti non vengano in possesso di informazioni privilegiate;
 - iii. ove abbia il ragionevole sospetto che una o più informazioni privilegiate siano state trasmesse a terzi non autorizzati a riceverle, attiva le procedure che regolano i casi di comunicazione non autorizzata a terzi.

Documenti di riferimento:

- Procedura - Gestione Registro dei soggetti aventi accesso alle informazioni privilegiate
- Procedura di gestione delle informazioni privilegiate
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice di comportamento in materia di informazione societaria al mercato

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato e del CFO in appositi armadi chiusi, ovvero se telematica, accessibile mediante credenziali note solo al Presidente, all'Amministratore Delegato ed al Dirigente Preposto.

12.9 Gestione della clientela

- ✓ **Potere decisionale:** Presidente, Amministratore Delegato e Direttore Generale
- ✓ **Potere di gestione:** Team di riferimento responsabile delle procedure di *Advisory* ed *Equity* e Assistenza alla Direzione, per la gestione degli aspetti operativi e amministrativi dell'apertura dei rapporti con la clientela
- ✓ **Potere di controllo:** Presidente, Amministratore Delegato e Direttore Generale non

coinvolto nella gestione dello specifico cliente

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione della clientela da parte di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso

- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{ter} c.p., Corruzione in atti giudiziari
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

- ❖ i reati societari, previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2637 c.c., Aggiotaggio
 - Art. 2635 c.c., Corruzione tra privati
 - Art. 2635^{bis} c.c., Istigazione alla corruzione tra privati

- ❖ i reati con finalità di terrorismo o di eversione dell'ordine democratico, previsti dall'art. 25^{quater} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 270^{bis} c.p., Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

- ❖ i reati di abusi di mercato, previsti dall'art. 25^{sexies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
 - Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria

- ❖ i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, previsti dall'art. 25^{octies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 648 c.p., Ricettazione
 - Art. 648^{bis} c.p., Riciclaggio
 - Art. 648^{ter} c.p., Impiego di denaro, beni o utilità di provenienza illecita
 - Art. 648^{ter.1} c.p., Autoriciclaggio

Regolamentazione: il processo è differenziato a seconda che si tratti di una operazione di *Advisory* o di *Investimento*:

A) Clienti per operazioni di *Advisory*

L'attività di *Advisory* consiste un servizio di assistenza in operazione di finanza straordinaria prestato a società terze.

Prima di procedere all'apertura di un rapporto di *Advisory*, l'Ufficio di Segreteria, o il CFO, consultando internet o appositi date base verificano preliminarmente se la società cliente abbia qualsivoglia legame con associazioni criminali o terroristiche.

Nel caso in cui l'esito di tale verifica risultasse positivo, il Presidente o l'Amministratore Delegato o il Direttore Generale rifiuteranno l'incarico.

Nel caso in cui l'esito di tale verifica risultasse negativo, a seguito degli accordi intercorsi tra le parti, il Presidente o l'Amministratore Delegato o il Direttore Generale redige e sottoscrive l'incarico per formalizzare l'oggetto e gli aspetti principali del servizio nonché le relative condizioni economiche.

B) Operazioni di investimento

L'attività di *investimento* consiste nell'acquisizione di partecipazioni nel capitale di società quotate e non quotate.

Il Presidente o l'Amministratore Delegato o il Direttore Generale valutano l'opportunità economica dell'operazione di investimento e decidono se, come e quando procedere con il progetto di investimento nel capitale di una società terza.

L'Ufficio di Segreteria o il CFO effettuano, anche in questo caso, i controlli preliminari sull'eventuale appartenenza della società terza ad associazioni criminali o terroristiche.

Nel caso in cui l'esito di dette verifiche fosse positivo, l'addetto all'Ufficio Segreteria effettua ulteriori controlli, preliminari rispetto alla decisione finale, in materia di "*prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo*", informando tempestivamente il Presidente, ovvero l'Amministratore Delegato, delle risultanze. Nell'ipotesi in cui l'accertamento fosse positivo ed emergessero, dunque, fondati sospetti sulla controparte e/o gli obiettivi dalla stessa perseguiti con l'operazione, il Presidente, ovvero l'Amministratore Delegato, deliberano di non procedere oltre. Diversamente, ove non via siano fondati sospetti, ma residuino comunque profili meritevoli di attenzione, il Presidente – su richiesta del soggetto coinvolto - fornisce un'adeguata informativa al Consiglio di Amministrazione, prima di procedere con la realizzazione dell'operazione, affinché lo stesso assuma le decisioni ritenute più opportune a tutela della Società.

Nel caso in cui l'esito di dette verifiche fosse negativo, in assenza di pregiudiziali, si prosegue nell'iter di realizzazione dell'operazione.

Ulteriori controlli sulla correttezza delle operazioni di Investimento sono effettuati dall'Internal Audit e dall'Organismo di Vigilanza.

C) Operazioni di disinvestimento

L'attività di *Equity* consiste anche nella cessione di partecipazioni detenute da TIP in società quotate o non quotate.

Il Presidente, l'Amministratore Delegato ed Direttore Generale in accordo valutano l'opportunità economica dell'operazione di disinvestimento e decidono se, come e quando procedere.

L'Ufficio di Segreteria o il CFO nel caso di cessione di società non quotate a controparti non quotate effettuano, anche in questo caso, i controlli preliminari sull'eventuale appartenenza della società terza ad associazioni criminali o terroristiche.

Nel caso in cui l'esito di tali verifiche risultasse positivo, l'addetto all'Ufficio Segreteria effettua i controlli preliminari in materia di *"prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminali e di finanziamento del terrorismo"*, informando tempestivamente il Presidente, ovvero l'Amministratore Delegato, delle risultanze.

Nell'ipotesi in cui l'accertamento fosse positivo ed emergessero, dunque, fondati sospetti sulla controparte e/o gli obiettivi dalla stessa perseguiti con l'operazione, il Presidente, ovvero l'Amministratore Delegato, deliberano di non procedere oltre. Diversamente, ove non via siano fondati sospetti, ma residuino comunque profili meritevoli di attenzione, il Presidente – su richiesta del soggetto coinvolto - fornisce un'adeguata informativa al Consiglio di Amministrazione, prima di procedere con la realizzazione dell'operazione, affinché lo stesso assuma le decisioni ritenute più opportune a tutela della Società.

Nel caso in cui l'esito di dette verifiche fosse negativo, in assenza di pregiudiziali, si prosegue nell'iter di realizzazione dell'operazione.

Ulteriori disposizioni in materia di prevenzione dei reati di cui agli art. 184 e 185 TUF

La fase di sottoscrizione dell'incarico (di Advisory), ovvero la fase di definizione di un'operazione di investimento/ o disinvestimento sono gestite dal team di riferimento e controllate da chi tra Presidente, Amministratore Delegato o Direttore Generale non è coinvolto nell'operazione.

Controlli sulla correttezza delle operazioni di *Equity* sono effettuati inoltre anche dall'Internal Audit e dall'Organismo di Vigilanza.

Documenti di riferimento:

- Procedura - Gestione degli adempimenti per la prevenzione del finanziamento del terrorismo e della criminalità organizzata
- Procedura - Risk Client Evaluation
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Clienti e Fornitori
- Codice Etico Informatico
- Procedura - Gestione Registro dei soggetti aventi accesso alle informazioni privilegiate
- Codice di comportamento in materia di informazione societaria al mercato
- Procedura di gestione delle informazioni privilegiate

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via email, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo all'Amministratore Delegato e al Presidente.

12.10 Selezione e gestione dei fornitori

- ✓ **Potere decisionale:** Amministratore Delegato
- ✓ **Potere di gestione:** Assistente alla Direzione
- ✓ **Potere di controllo:** Internal Audit o Collegio Sindacale

Scopo: il presente protocollo ha lo scopo di definire le modalità di selezione e gestione dei fornitori di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{ter} c.p., Corruzione in atti giudiziari
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- ❖ i reati societari, previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2635 c.c., Corruzione tra privati
 - Art. 2635^{bis} c.c., Istigazione alla corruzione tra privati
- ❖ i reati con finalità di terrorismo o di eversione dell'ordine democratico, previsti dall'art. 25^{quater} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 270^{bis} c.p., Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

- ❖ i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, previsti dall'art. 25^{octies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 648^{ter} c.p., Impiego di denaro, beni o utilità di provenienza illecita
 - Art. 648^{ter}.1 c.p., Autoriciclaggio
- ❖ i reati in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, previsti dall'art. 25^{decies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 377^{bis} c.p., Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Regolamentazione: il processo in esame si suddivide in macrofasi:

1. Individuazione del rapporto contrattuale e selezione della controparte (eventuale);
 2. Trattativa e stipula del contratto;
 3. Esecuzione della prestazione contrattuale;
 4. Pagamento;
 5. Verifiche.
1. L'Amministratore Delegato individua la necessità di avviare determinati rapporti contrattuali con fornitori o eventuali altre controparti, anche estere, sulla base di esigenze di i prodotti, servizi. Per importi superiori a 5.000 euro vengono selezionati almeno 2 (due) possibili fornitori che, sono obbligati a presentare dei preventivi scritti. In caso di inottemperanza, è necessario fornire giustificazione scritta. Sulla base dei preventivi presentati, l'Amministratore Delegato individua il fornitore preferibile. Si precisa che la scelta deve basarsi esclusivamente su considerazioni economiche e di mercato, prediligendo le controparti che garantiscano il miglior rapporto qualità/prezzo, sull'apprezzamento che i possibili fornitori abbiano sul mercato e sulla loro capacità di far fronte agli obblighi normativi vigenti (es. sicurezza sul lavoro, privacy), ovvero a qualsivoglia criterio che non sia correlabile a interessi non legali o comunque ai limiti della legalità e dell'etica. In nessun modo si deve dare priorità a un fornitore che abbia un prezzo sensibilmente inferiore a quello di mercato laddove non si abbiano garanzie sul rispetto da parte dello stesso della normativa di riferimento.
 2. I fornitori devono fornire all'Amministratore Delegato la documentazione afferente la propria regolarità tecnica, amministrativa e normativa, per il tramite dell'Assistente alla Direzione, affinché questi provveda alla qualifica degli stessi. Inoltre, in caso di prodotti coperti da diritto d'autore, i fornitori devono produrre apposita documentazione che risponda alla tutela dello stesso. L'Amministratore Delegato stipula l'accordo contrattuale e l'Assistente alla Direzione invia l'ordine al fornitore.
 3. L'Amministratore Delegato si occupa della fase esecutiva del contratto.
 4. L'Amministratore Delegato previa verifica del contenuto della fornitura rispetto al preventivo approvato verifica da effettuarsi da parte del CFO, da l'autorizzazione a procedere al pagamento della prestazione ricevuta secondo i termini contrattuali, previa ricezione della fattura.
 5. L'Amministratore Delegato svolge i controlli sulla correttezza delle procedure, sulla rispondenza del rapporto contrattuale con le esigenze evidenziate sull'esecuzione delle previsioni contrattuali. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, informa sia l'*Internal Audit* che

il Collegio Sindacale.

Documenti di riferimento:

- Procedura Spese
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Codice Etico Clienti e Fornitori

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali.

12.11 Selezione e gestione dei consulenti

- ✓ **Potere decisionale: Presidente o Amministratore Delegato**
- ✓ **Potere di gestione: Amministratore Delegato**
- ✓ **Potere di controllo: Consiglio di Amministrazione**

Scopo: il presente protocollo ha lo scopo di definire le modalità di selezione e gestione dei consulenti di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di criminalità organizzata, previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione, previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{ter} c.p., Corruzione in atti giudiziari
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- ❖ i reati societari, previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2635 c.c., Corruzione tra privati

- Art. 2635*bis* c.c., Istigazione alla corruzione tra privati
- ❖ i reati con finalità di terrorismo o di eversione dell'ordine democratico, previsti dall'art. 25*quater* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 270*bis* c.p., Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico
- ❖ i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, previsti dall'art. 25*octies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 648*ter* c.p., Impiego di denaro, beni o utilità di provenienza illecita
 - Art. 648*ter*.1 c.p., Autoriciclaggio
- ❖ i reati in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, previsti dall'art. 25*decies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 377*bis* c.p., Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Regolamentazione: il processo in esame si suddivide in macrofasi:

1. Individuazione del rapporto contrattuale e selezione della controparte (eventuale);
 2. Trattativa e stipula del contratto;
 3. Esecuzione della prestazione contrattuale;
 4. Pagamento;
 5. Verifiche.
1. L'Amministratore Delegato o il Presidente individuano la necessità di avviare determinati rapporti contrattuali con consulenti in base alle esigenze operative. L'Amministratore Delegato seleziona almeno 2 possibili consulenti che siano competenti nella materia di riferimento, i quali per servizi di importi superiori a 5.000 euro hanno l'obbligo, salvo giustificazione per iscritto di eventuale deroga, di presentare un preventivo scritto. L'Amministratore Delegato individua il consulente preferibile sulla base delle competenze emerse, tenuto conto del rapporto fiduciario necessario e dei criteri di economicità. Si precisa che in nessun caso è consentito svolgere consulenze non necessarie o attraverso la selezione di specifici consulenti, al fine di ottenere vantaggi illeciti per la società, siano essi economici o di altra natura, ovvero attuare favoritismi o vantaggi per terzi.
 2. Per la sola fase di trattativa e stipula, dunque per la fase gestoria, l'Amministratore Delegato propone il consulente prescelto al Presidente al fine di procedere alle trattative finalizzate alla stipula dell'accordo contrattuale.
 3. L'Amministratore Delegato si occupa della fase esecutiva del contratto.
 4. L'Amministratore Delegato procede al pagamento della prestazione ricevuta secondo i termini contrattuali, previa ricezione della fattura.
 5. L'Amministratore Delegato svolge i controlli sulla correttezza delle procedure, sulla rispondenza del rapporto contrattuale con le esigenze evidenziate sull'esecuzione delle previsioni contrattuali. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, l'Amministratore Delegato informa sia l'Organismo di Vigilanza che il Consiglio di Amministrazione.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Codice Etico Clienti e Fornitori
- Procedura Spese

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note anche al Presidente nei termini di legge.

12.12 Selezione, assunzione e gestione del personale e degli adempimenti relativi al trattamento previdenziale

- ✓ **Potere decisionale: Presidente e Amministratore Delegato**
- ✓ **Potere di gestione: Addetto all'Ufficio di Segreteria (solo per gli adempimenti operativi)**
- ✓ **Potere di controllo: Direttore Generale**

Scopo: il presente protocollo ha lo scopo di definire le modalità di selezione e assunzione del personale di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ **i reati in materia di criminalità organizzata,** previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ **i reati in materia di concussione, induzione indebita a dare o promettere utilità e corruzione,** previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{ter} c.p., Corruzione in atti giudiziari
 - Art. 319^{quater} c.p., Induzione indebita a dare o promettere utilità
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- ❖ **i reati societari,** previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2635 c.c., Corruzione tra privati

- Art. 2635*bis* c.c., Istigazione alla corruzione tra privati
- ❖ i reati con finalità di terrorismo o di eversione dell'ordine democratico, previsti dall'art. 25*quater* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 270*bis* c.p., Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico
- ❖ i reati contro la personalità individuale, previsti dall'art. 25*quinqüies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 600 c.p., Riduzione o mantenimento in schiavitù o in servitù
 - Art. 601 c.p., Tratta di persone
 - Art. 602 c.p., Acquisto e alienazione di schiavi
 - Art. 603*bis* c.p., Intermediazione illecita e sfruttamento del lavoro
- ❖ i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, previsti dall'art. 25*octies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 648*ter* c.p., Impiego di denaro, beni o utilità di provenienza illecita
 - Art. 648*ter*.1 c.p., Autoriciclaggio
- ❖ i reati in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, previsti dall'art. 25*decies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 377*bis* c.p., Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- ❖ i reati in materia di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, previsti dall'art. 25*duodecies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 22, Lavoro subordinato a tempo determinato e indeterminato, D.lgs. n. 286/1998, Testo unico sull'immigrazione

Regolamentazione: nell'ambito di tale processo vengono di seguito definiti ruoli e responsabilità dei soggetti incaricati di gestire le diverse fasi, nonché i protocolli di prevenzione che da questi devono essere applicati. In particolare, il processo viene descritto distinguendo le seguenti attività:

- Selezione del personale da inserire nelle aree *core business* della Società);
- Selezione del personale da inserire nelle attività di supporto.

Le attività inerenti la selezione e assunzione del personale vengono condotte direttamente dall'Amministratore Delegato, con l'ausilio dell'Addetto all'Ufficio di Segreteria, con l'obiettivo di assicurare che il processo di assunzione sia motivato da effettive necessità aziendali, che sia condotto in maniera trasparente e documentabile e che sia basato su criteri non arbitrari e quanto più possibile oggettivi. Tale processo si articola nelle seguenti fasi:

- Identificazione dell'esigenza di assunzione personale: il Presidente, l'Amministratore Delegato e il Direttore Generale, nel caso emerga la necessità di ampliare l'organico aziendale, valutano e decidono la necessità di avvalersi di nuove risorse e le competenze richieste.
- Selezione delle candidature: l'Amministratore Delegato, una volta ottenuta e analizzata la rosa di

candidati a ricoprire il ruolo ricercato, provvede ad effettuare un colloquio conoscitivo. Nel corso dell'iter di selezione devono essere accertati e valutati i rapporti, diretti o indiretti, tra il candidato e la Pubblica Amministrazione, che vengono formalizzati tramite scheda informativa compilata dal candidato ovvero i suoi requisiti di onorabilità e professionalità (se richiesti per la mansione specifica).

In caso di esito positivo, solo per la selezione del personale da inserire nelle aree *core business* della Società, il candidato sostiene una prova scritta. Tale prova è valutata dall'Amministratore Delegato unitamente al Direttore Generale.

Le valutazioni formalizzate dei candidati, unitamente alla scheda informativa, sono archiviate da parte dell'Amministratore Delegato.

- Assunzione del candidato e inserimento in azienda: l'Amministratore Delegato, all'esito della selezione, ricevuta l'approvazione dal Presidente o dal Direttore Generale, provvede all'espletamento di tutte le pratiche connesse all'assunzione del candidato.

In caso di assunzione di personale appartenente a paesi terzi, verrà effettuata una specifica verifica della regolarità del permesso di soggiorno presso il territorio italiano, avvalendosi, eventualmente, del supporto della società che gestisce in *outsourcing* gli adempimenti del personale.

L'addetta alla Segreteria di Direzione provvede a consegnare al neoassunto copia di tutte le procedure, della modulistica in essere nonché del Codice Etico e del Modello di organizzazione, gestione e controllo della Società richiedendone l'adesione. La dichiarazione di adesione è archiviata presso l'Amministratore Delegato, unitamente al contratto di assunzione. Le lettere di assunzione vengono firmate dall'Amministratore Delegato o dal Presidente. Si precisa che il personale è tenuto a svolgere, in corrispondenza con l'assunzione, la formazione prevista dalla normativa in materia di sicurezza sui luoghi di lavoro, nonché su tematiche ambientali che impattino sul proprio operato e sull'utilizzo corretto degli strumenti informatici.

Si demandano direttamente all'Amministratore Delegato, con l'ausilio dei consulenti del lavoro, le seguenti incombenze e adempimenti o procedure:

- a. gestione delle attività legate alla predisposizione dei cedolini e dei modelli per il pagamento di oneri fiscali, sociali e previdenziali;
- b. gestione degli adempimenti legati all'assunzione di personale appartenente a categorie protette (eventuale).

Documenti di riferimento:

- Procedura - Selezione e assunzione del personale
- Regolamento disciplinare aziendale per gli addetti alle attività di *investment/merchand bank*
- Regolamento disciplinare aziendale per il personale di segreteria
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note anche Presidente, nei termini di legge.

12.13 Gestione delle c.d. informazioni privilegiate e manipolazione del mercato

- ✓ **Potere decisionale: Presidente**
- ✓ **Potere di gestione: Amministratore Delegato**
- ✓ **Potere di controllo: Consiglio di Amministrazione**

Scopo: il presente protocollo ha lo scopo di definire le modalità trattamento delle informazioni privilegiate acquisite da TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati di abusi di mercato previsti dall'art. 25^{sexies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
- ❖ Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
- ❖ Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria.

Regolamentazione per la gestione delle informazioni privilegiate (art. 184 TUF):

In ottemperanza alle disposizioni della *Market Abuse Regulation* (o “MAR”) le informazioni privilegiate vengono gestite da TIP secondo il seguente processo:

Il Presidente individua le specifiche informazioni che possono assumere, anche in un secondo momento, natura privilegiata (cd. “informazioni rilevanti”).

L'Amministratore Delegato monitora la circolazione delle specifiche informazioni rilevanti, anche utilizzando la *Relevant Information List* (cd. “RIL”), individua il momento in cui la specifica informazione rilevante diviene privilegiata e segrega l'informazione privilegiata medesima attivando l'*Insider List*. L'informazione segregata è oggetto di specifiche regole in merito alla sua circolazione sia all'interno, sia all'esterno della Società.

Trovano applicazione le misure di separazione organizzativa previste tempo per tempo.

Su proposta dell'Amministratore Delegato, il Presidente decide se pubblicare l'informazione privilegiata immediatamente o deferire la stessa. Nel caso in cui si opti per la pubblicazione dell'informazione, l'Amministratore Delegato procede in tal senso. In alternativa, il medesimo avvia il monitoraggio delle condizioni che consentano il ritardo della pubblicazione. Al venir meno di tali condizioni, l'Amministratore Delegato procede alla pubblicazione dell'informazione.

Il Consiglio di Amministrazione vigila sulle attività poste in essere dall'Amministratore Delegato e sul potere esercitato dal Presidente, richiedendone, ogni qual volta lo ritenga opportuno, chiarimenti sulle decisioni intraprese e monitorando, anche a campione, la gestione delle singole informazioni.

Ai fini della gestione delle informazioni privilegiate, i destinatari – che entrino eventualmente in possesso di informazioni privilegiate – sono tenuti al rispetto delle prescrizioni sancite nel Manuale delle Procedure Aziendali e nel Codice Etico, nonché delle seguenti previsioni:

- ❖ i destinatari possono comunicare le informazioni privilegiate di cui sono venuti in possesso, nell'esercizio del proprio lavoro, della professione, della funzione, o dell'ufficio esclusivamente:
 - a soggetti interni alla Società che hanno necessità di conoscerle per motivi anch'essi attinenti al normale esercizio del proprio lavoro, evidenziando la natura riservata delle informazioni;

- a soggetti terzi, esterni alla Società, che hanno necessità di conoscerle per un motivo attinente allo svolgimento del lavoro, della professione, della funzione o dell'ufficio svolto da tali soggetti;
- ❖ la comunicazione delle informazioni privilegiate ai soggetti esterni deve comunque avvenire nel rispetto degli obblighi di riservatezza;
- ❖ è inibito l'accesso a tali informazioni da parte di persone diverse da quelle che le gestiscono o vi accedono in ragione delle funzioni svolte presso la, o per conto della, Società;
- ❖ è impedita la circolazione impropria, anche accidentale, di tali informazioni all'interno della Società. In particolare i documenti contenenti informazioni privilegiate o destinate a diventare tali, devono essere conservati in luoghi – anche informatizzati - ad accesso limitato e adeguatamente presidiati. Eventuali copie in eccesso dei documenti contenenti informazioni privilegiate devono essere distrutte al termine di eventuali riunioni;
- ❖ è imposto il rispetto del dovere di massima riservatezza, all'interno e all'esterno della Società;
- ❖ in caso di legittima comunicazione dell'informazione privilegiata a soggetti esterni alla Società, devono essere predisposte clausole contrattuali che vincolino la parte terza alla riservatezza dell'informazione, eventualmente prevedendo l'adozione, da parte di tali soggetti, di idonee misure di protezione dell'informazione ricevuta;
- ❖ è vietato acquistare, vendere o compiere altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni privilegiate di cui si è in possesso;
- ❖ è vietato raccomandare ad altri il, o indurre altri al, compimento di taluna delle operazioni indicate a punto precedente sulla base delle informazioni privilegiate di cui si è in possesso.

Ai destinatari è espressamente richiesto di:

- assicurare la massima riservatezza riguardo ai documenti e alle informazioni eventualmente acquisite nello svolgimento dei propri compiti e funzioni, rispettando le previsioni aziendali in materia di trattamento delle informazioni privilegiate;
- agire con correttezza e con la massima trasparenza e professionalità in occasione della predisposizione e diffusione di ogni comunicazione istituzionale al mercato e al pubblico in generale;
- assicurare l'accuratezza e la veridicità di ogni informazione diffusa al mercato e al pubblico in generale;
- porre in essere operazioni personali nel rispetto delle norme interne (Codice Internal Dealing);
- monitorare adeguatamente l'esecuzione delle funzioni esternalizzate, al fine di verificare che siano gestite in conformità alla normativa applicabile e alle previsioni della delega conferita;
- verificare che gli *outsourcer* garantiscano la protezione e la corretta gestione delle informazioni riservate relative alla Società e ai suoi clienti;
- segnalare senza indugio all'Organismo di Vigilanza ogni violazione delle previsioni interne e di legge in materia di gestione delle informazioni privilegiate.

Ai destinatari è inoltre espressamente fatto divieto di:

- sollecitare l'ottenimento di informazioni privilegiate su strumenti finanziari o emittenti strumenti finanziari quotati, salvo che in base ad accordi contrattuali o ai sensi della normativa applicabile;

- acquistare direttamente o tramite terzi uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere informazioni fuorvianti sullo strumento finanziario in modo da alterarne il prezzo;
- effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che lo stesso non venga esplicitato nelle forme previste dalle previsioni interne e di legge applicabili), allorché tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;
- impartire ordini di compravendita o eseguire operazioni prima della diffusione da parte della Società di informazioni privilegiate;
- comunicare o diffondere all'esterno informazioni, studi o valutazioni sulla Società che possano influenzare i terzi, beneficiando di conseguenza degli effetti sul prezzo di detto strumento.

Tracciabilità: tutte le fasi del processo di gestione delle informazioni privilegiate devono essere documentate. L'Insider List è tempestivamente aggiornata. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo allo stesso ed al Presidente.

Documenti di riferimento:

- Procedura di gestione delle informazioni privilegiate
- Procedura di gestione del registro dei soggetti aventi accesso alle informazioni privilegiate
- Codice di comportamento in materia di informazione societaria al mercato
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Codice Etico Clienti e Fornitori

Regolamentazione per la prevenzione degli abusi di mercato (art. 185 TUF)

I destinatari, nel compimento di operazioni di investimento o disinvestimento per conto della Società su strumenti finanziari di cui all'art. 180 TUF (avendo particolare riguardo a quelli emessi della Società stessa, ovvero emessi da un emittente per il quale la Società sta prestando la propria attività), dovranno astenersi dal:

- compiere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo degli strumenti finanziari;
- compiere operazioni o ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo degli strumenti finanziari;
- compiere operazioni o ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato degli strumenti finanziari ad un livello anomalo o artificiale;
- acquistare, anche di concerto con altri, una posizione dominante sull'offerta o sulla domanda dello strumento finanziario con la consapevolezza che così facendo si potranno fissare direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;

- prendere posizione su uno strumento finanziario e/o diffondere valutazioni sullo strumento finanziario, o sul suo emittente, con la consapevolezza che così facendo si potrà beneficiare dell'impatto della valutazione diffusa sul prezzo dello strumento finanziario;
- compiere operazioni di acquisto/vendita, soprattutto se rappresenta una quota significativa della negoziazione giornaliera dello strumento finanziario, con la consapevolezza che così facendo si potrà ottenere una significativa variazione del prezzo dello strumento finanziario ovvero dello strumento derivato collegato o dell'attività sottostante ammessi alla negoziazione;
- effettuare operazioni di acquisto/vendita senza che si determini alcuna variazione nella, ovvero alcun trasferimento effettivo della, proprietà dello strumento finanziario interessato;
- acquistare o vendere gli strumenti finanziari alla chiusura del mercato con la consapevolezza che così facendo si potranno ingannare gli investitori che operano sulla base dei prezzi di chiusura;
- concentrare operazioni di acquisto/vendita in un breve lasso di tempo con la consapevolezza che così facendo si potrà ottenere una variazione del prezzo che successivamente si potrà invertire;
- effettuare operazioni di acquisto/vendita che prevedono inversioni di posizioni in acquisto o in vendita nel breve periodo, soprattutto se rappresentano una quota significativa del volume giornaliero degli scambi dello strumento finanziario, con la consapevolezza che così facendo si potranno ottenere significative variazioni di prezzo;
- trasmettere ordini di acquisto/vendita senza l'intenzione di eseguirli, con la consapevolezza che così facendo si potranno fornire indicazioni fuorvianti circa l'esistenza di una domanda/offerta a prezzi elevati/bassi;
- concentrare operazioni di acquisto/vendita intorno ai momenti utili per il calcolo dei prezzi di apertura o di chiusura, di quelli di controllo, di riferimento, di regolamento o di valutazione, con la consapevolezza che così facendo si potranno variare tali prezzi.

Documenti di riferimento:

- Procedura di gestione delle informazioni privilegiate
- Codice di comportamento in materia di informazione societaria al mercato
- Codice Etico

Tracciabilità: tutte le fasi del processo che porta alle decisioni di compravendita o di cessione sono opportunamente documentate e tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo allo stesso ed al Presidente.

12.14 Gestione dei doni e regalie ricevuti dai dipendenti

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Soggetto coinvolto**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei doni e delle regalie ricevute dai dipendenti di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati societari previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2635 c.c., Corruzione tra privati
 - Art. 2635^{bis} c.c., Istigazione alla corruzione tra privati

Regolamentazione: la gestione dei doni e delle regalie ricevuti dai dipendenti deve avvenire nel rispetto della legge e delle direttive aziendali, nei limiti della correttezza e adeguatezza, nel rispetto dei principi di segregazione delle funzioni, tracciabilità dei processi ed evidenza controlli ritenuti idonei ad evitare creazione di sponsorizzazioni che celino fini corruttivi o atti a realizzare favoritismi illeciti ovvero circolazione di contante non autorizzata.

In caso di ricezione di benefici non di modico valore, i dipendenti informano per iscritto l'Amministratore Delegato per le valutazioni di competenza. E', invece, vietato accettare o effettuare omaggi in denaro.

E' consentita, in ogni caso, l'effettuazione o la ricezione di regali di modico valore elargiti su base di prassi comunemente accettate (es. regali natalizi), così come gli atti di cortesia commerciale, quando siano di modico valore e tali da non compromettere l'integrità e la reputazione di una delle parti e da non poter essere interpretati, da un osservatore imparziale, come finalizzati ad acquisire un vantaggio in modo improprio.

Il Presidente ha il compito di controllare se i benefici in questione possano costituire potenziale conflitto con i doveri dei dipendenti verso la Società o i clienti o siano finalizzati ad ottenere vantaggi impropri.

Documenti di riferimento:

- Regolamento disciplinare Segreteria
- Regolamento disciplinare per gli addetti alle attività di *investment/merchand bank*
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note anche al Presidente, nei termini di legge. In caso di assenza di evidenza documentale, è predisposta verbalizzazione di quanto accaduto dal soggetto coinvolto, sottoscritta per l'approvazione dall'Amministratore Delegato.

12.15 Utilizzo di opere di ingegno coperte dal diritto d'autore

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Assistente alla Direzione**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione delle opere di ingegno coperte dal diritto d'autore utilizzate da TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di violazione del diritto d'autore previsti dall'art. 25^{novies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 171, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171^{bis}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio.
 - Art. 171^{ter}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171^{septies}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171^{octies}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Regolamentazione: il processo si articola nelle seguenti macrofasi:

1. Individuazione dell'utilizzo di un'opera d'ingegno coperta dal diritto d'autore;
2. Identificazione delle condizioni di utilizzo;
3. Verifiche.

1. Nell'ambito delle attività aziendali, è possibile l'utilizzo di opere di ingegno coperte dal diritto d'autore.

2. Ciascun utente è tenuto a conformarsi alle previsioni aziendali in materia, elaborate in un documento con la cooperazione tra l'Amministratore Delegato e il Presidente anche in ordine alla verifica del rispetto delle previsioni normative. Tale documento deve prevedere inibizioni all'utilizzo improprio dell'opera di ingegno e stabilire misure di richiamo in caso di violazioni. Deve essere comunicato mediante circolare interna, reso noto in sede di assunzione e messo a disposizione nella bacheca aziendale.

3. Il Presidente effettua i controlli sulla correttezza delle procedure, sulla rispondenza del rapporto contrattuale con le esigenze evidenziate, sull'esecuzione delle previsioni contrattuali. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, il Consiglio di Amministrazione.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note allo stesso ed al Presidente.

12.16 Utilizzo dei sistemi informatici da parte degli utenti

- ✓ **Potere decisionale:** Presidente, Amministratore Delegato,
- ✓ **Potere di gestione:** Utente

✓ **Potere di controllo: Responsabile IT, Soggetti esterni regolarmente incaricati dalla Società**

Scopo: il presente protocollo ha lo scopo di definire le modalità di utilizzo dei sistemi informatici da parte degli utenti di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati informatici e di trattamento illecito di dati previsti dall'art. 24**bis** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 615**ter** c.p., Accesso abusivo ad un sistema informatico o telematico
 - Art. 617**quater** c.p., Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
 - Art. 617**quinquies** c.p., Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
 - Art. 635**bis** c.p., Danneggiamento di informazioni, dati e programmi informatici
 - Art. 635**quater** c.p., Danneggiamento di sistemi informatici o telematici
 - Art. 615**quater** c.p., Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
 - Art. 615**quinquies** c.p., Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- ❖ i reati di criminalità organizzata previsti dall'art. 24**ter** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere
 - Art. 416**bis** c.p., Associazioni di tipo mafioso anche straniere
- ❖ i reati contro la personalità individuale previsti dall'art. 25**quinquies** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 600**quater.1** c.p., Pornografia virtuale
 - Art. 609**undecies** c.p., Adescamento di minorenni
- ❖ i reati di abusi di mercato previsti dall'art. 25**sexies** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
 - Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria

Regolamentazione: l'utilizzo dei sistemi informatici e telematici deve avvenire nel rispetto della legge e delle direttive aziendali, nei limiti della correttezza e adeguatezza. Il *pc* ed i telefoni aziendali sono uno strumento di lavoro e ogni utilizzo non inerente l'attività lavorativa è vietato.

Il Presidente e l'Amministratore Delegato approvano un regolamento informatico per l'esercizio delle attività aziendali, che ogni utente è tenuto a rispettare.

Ogni Utente è tenuto a impedire l'accesso al proprio pc da parte di soggetti non autorizzati, ovvero consentire l'accesso a terzi incaricati, nei limiti dell'incarico conferito.

L'accesso alla rete e ai relativi servizi di rete deve avvenire solamente mediante autenticazione del soggetto, avvalendosi di credenziali di autenticazione. Ogni utente deve custodire le proprie credenziali di accesso in modo tale da non permetterne la conoscenza, anche occasionale, a terzi.

Nessun dipendente è autorizzato a modificare le impostazioni del proprio pc. In particolare non è consentito l'uso di programmi diversi da quelli ufficialmente installati.

L'accesso a internet e l'utilizzo della posta elettronica sono consentiti nei limiti degli scopi attinenti al proprio lavoro. E' obbligatorio porre la massima attenzione nell'aprire allegati di posta elettronica prima del loro utilizzo. In caso di individuazione di avvisi o documenti sospetti, l'utente è tenuto ad informare tempestivamente il Responsabile del trattamento dei dati, che svolge le verifiche del caso, avvalendosi anche di personale esterno.

L'utilizzo non consentito (a titolo meramente esemplificativo, l'installazione di un programma *software* non previsto per lo svolgimento delle attività lavorative) deve essere necessariamente segnalato mediante apposito avviso di sistema all'Amministratore Delegato, che è tenuto a informare per gli adempimenti tecnici operativi l'Amministratore di Sistema. In tal modo è possibile la tracciabilità delle operazioni non consentite, senza violazione dei principi di legge individuati dalla L. 300/1970 e D.lgs. n. 196/2003.

E' vietata qualsiasi alterazione di registri informatici, documentazione fiscale, nonché eventuali interventi di danneggiamento o *hackeraggio* verso sistemi informatici interni o di terzi.

L'Amministratore Delegato, anche avvalendosi di persone competenti - come il Responsabile IT o soggetti esterni regolarmente incaricati dalla Società - è tenuto a verificare eventuali utilizzi non consentiti da parte degli utenti.

Documenti di riferimento:

- Regolamento per la tutela delle informazioni riservate e il corretto utilizzo degli strumenti informatici di TIP
- Regolamento per l'attribuzione di telefono aziendale e sim
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico
- Procedura gestione registro dei soggetti aventi accesso alle informazioni privilegiate
- Procedura di gestione del registro dei soggetti aventi accesso alle informazioni privilegiate

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note anche al Presidente, nei termini di legge.

12.17 Utilizzo e gestione dei sistemi informatici da parte dell'Amministratore di Sistema e di utilizzatori di pc Administrator oppure utenti con accessi/permessi privilegiati

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Amministratore di Sistema/pc *Administrator* o Utente con accessi/permessi privilegiati**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di utilizzo e gestione dei sistemi informatici da parte degli Utenti di TIP con accessi e permessi privilegiati al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati informatici e di trattamento illecito di dati previsti dall'art. 24**bis** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 615**ter** c.p., Accesso abusivo ad un sistema informatico o telematico
 - Art. 617**quater** c.p., Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
 - Art. 617**quinqües** c.p., Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
 - Art. 635**bis** c.p., Danneggiamento di informazioni, dati e programmi informatici
 - Art. 635**quater** c.p., Danneggiamento di sistemi informatici o telematici
 - Art. 615**quater** c.p., Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
 - Art. 615**quinqües** c.p., Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

- ❖ i reati di criminalità organizzata previsti dall'art. 24**ter** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416**bis** c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)

- ❖ i reati di abusi di mercato previsti dall'art. 25**sexies** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
 - Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria

- ❖ i reati in materia di violazione del diritto d'autore previsti dall'art. 25**novies** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 171, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171**bis**, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio.
 - Art. 171**ter**, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171**septies**, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171**octies**, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Regolamentazione: l'utilizzo dei sistemi informatici e telematici deve avvenire nel rispetto della legge e delle direttive aziendali, nei limiti della correttezza e adeguatezza. Il pc è uno strumento di lavoro e ogni utilizzo non inerente l'attività lavorativa è vietato.

L'Amministratore Delegato conferisce incarico scritto all'Amministratore di Sistema, identificando le specifiche attività da svolgere, le finalità da perseguire e gli obblighi, con particolare attenzione alla non divulgazione delle informazioni apprese nello svolgimento del proprio incarico e a rispettare quanto contenuto nel presente Modello per le attività di sua competenza.

L'Amministratore di Sistema fornisce supporto tecnico sia al Amministratore Delegato che agli utenti, nei limiti dell'incarico conferito, ed esegue le direttive aziendali in ordine agli aggiornamenti, alla limitazione di accesso ai pc, alla rete, alla posta elettronica di ciascun utente e a internet. L'Amministratore di Sistema dietro indicazione dell'Amministratore Delegato inserisce inoltre misure di protezione dei documenti elettronici anche al fine di identificare i soggetti che vi operano.

L'Amministratore di Sistema custodisce le eventuali credenziali di accesso degli utenti note nonché le credenziali di accesso in qualità di Amministratore al fine di evitare la conoscenza o la divulgazione delle stesse. In caso di interruzione del rapporto lavorativo, l'Amministratore di Sistema prevede la rimozione dei diritti di accesso.

L'Amministratore di Sistema installa su pc degli utenti e ad uso aziendale esclusivamente programmi autorizzati dall'Amministratore Delegato.

L'Amministratore di Sistema gestisce la sicurezza rispetto a possibili intrusioni esterne per il tramite di un sistema *Firewall*, che controlla sia il traffico in ingresso che in uscita attraverso definite regole che impediscono intrusioni dall'esterno.

L'Amministratore di Sistema installa antivirus su ciascun pc presente in azienda.

L'Amministratore di Sistema attua controlli sulla rete aziendale e sulle informazioni che vi transitano nonché l'instradamento della rete al fine di evitare che siano violate le politiche di sicurezza nonché stabilisce procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.

L'Amministratore di Sistema informa l'Amministratore Delegato o il Presidente di ogni problematica aziendale o esigenze di ausili tecnici o aggiornamenti, i quali decidono in merito.

Qualora sia necessario avvalersi di personale tecnico esterno, l'Amministratore di Sistema informa l'Amministratore Delegato o il Presidente e, ottenuta l'autorizzazione, assiste l'intervento, verificando la corretta esecuzione della prestazione nei limiti dell'incarico conferito e fornendo esclusivamente le credenziali necessarie. Il Personale tecnico esterno è tenuto al rispetto della riservatezza e sottoscrive un impegno in tal senso.

Spetta al Presidente il controllo del rispetto delle previsioni individuate. In caso di utilizzi difformi o non autorizzati, e quando si tratti di condotte poste in essere in violazione delle prescrizioni, il Presidente dà informativa all'Organismo di Vigilanza.

Documenti di riferimento:

- Regolamento per la tutela delle informazioni riservate e il corretto utilizzo degli strumenti informatici di TIP
- Procedura di gestione del registro dei soggetti aventi accesso alle informazioni privilegiate
- Regolamento per l'attribuzione di telefono aziendale e sim
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via email, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo al medesimo.

12.18 Utilizzo di firma digitale

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Consulente esterno/Assistente alla Direzione – Amministratore Delegato**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di utilizzo della firma digitale che impegna l'Amministrazione di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati informatici e di trattamento illecito di dati previsti dall'art. 24**bis** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 635**bis** c.p., Danneggiamento di informazioni, dati e programmi informatici
 - Art. 635**quater** c.p., Danneggiamento di sistemi informatici o telematici

Regolamentazione: l'utilizzo della firma digitale deve avvenire nel rispetto della legge e delle direttive aziendali, nei limiti della correttezza e adeguatezza nonché degli incarichi conferiti.

L'utilizzo di tale strumento deve essere vincolato, necessariamente, all'inserimento di una credenziale di autenticazione/*password* di conoscenza e di uso esclusivo dell'effettivo titolare della firma, salvo espressa delega o procura specifica, avallata dall'Amministratore Delegato.

L'Amministratore Delegato verifica il corretto utilizzo della firma elettronica da parte dei soggetti autorizzati e nei limiti dell'impiego consentito. In caso di violazioni, informa tempestivamente il Consiglio di Amministrazione.

Documenti di riferimento:

- Regolamento per la tutela delle informazioni riservate e il corretto utilizzo degli strumenti informatici di TIP
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via email, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo allo stesso ed al Presidente.

12.19 Utilizzo della posta certificata

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Assistente alla Direzione - Amministratore Delegato**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di utilizzo della posta certificata di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati informatici e di trattamento illecito di dati previsti dall'art. 24**bis** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 635**bis** c.p., Danneggiamento di informazioni, dati e programmi informatici
 - Art. 635**quater** c.p., Danneggiamento di sistemi informatici o telematici
- ❖ i reati in materia di abusi di mercato, previsti dall'art. 25**sexies** del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 184, Abuso di informazioni privilegiate, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria
 - Art. 185, Manipolazione del mercato, D.lgs. n. 58/1998, Testo unico delle disposizioni in materia di intermediazione finanziaria

Regolamentazione: l'utilizzo della posta elettronica certificata deve avvenire nel rispetto della legge e delle direttive aziendali, nei limiti della correttezza e adeguatezza nonché degli incarichi conferiti.

L'utilizzo di tale strumento deve essere vincolato, necessariamente, all'inserimento di una credenziale di autenticazione/*password* di conoscenza e di uso esclusivo dell'effettivo titolare della firma.

Il Presidente verifica il corretto utilizzo della posta certificata da parte dei soggetti autorizzati e nei limiti dell'impiego consentito. In caso di violazioni, il Presidente informa tempestivamente l'Organismo di Vigilanza e il Consiglio di Amministrazione.

Documenti di riferimento:

- Regolamento per la tutela delle informazioni riservate e il corretto utilizzo degli strumenti informatici di TIP
- Procedura gestione registro dei soggetti aventi accesso alle informazioni privilegiate
- Procedura di gestione del registro dei soggetti aventi accesso alle informazioni privilegiate
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo al medesimo al Presidente ed alla Segreteria di Direzione.

12.20 Smarrimento di strumenti informatici

- ✓ **Potere decisionale: Amministratore Delegato**
- ✓ **Potere di gestione: Soggetto coinvolto**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di reazione allo smarrimento degli strumenti informatici dati in dotazione da TIP ai suoi dipendenti al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ **i reati informatici e di trattamento illecito di dati** previsti dall'art. 24*bis* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 635*bis* c.p., Danneggiamento di informazioni, dati e programmi informatici
 - Art. 635*quater* c.p., Danneggiamento di sistemi informatici o telematici
- ❖ **i reati in materia di violazione del diritto d'autore** previsti dall'art. 25*novies* del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 171, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171*bis*, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio.
 - Art. 171*ter*, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171*septies*, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171*octies*, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Regolamentazione: l'utilizzo di strumenti informatici, quali pc portatili, telefoni cellulari, tablet, deve avvenire nel rispetto della legge e delle direttive aziendali, nei limiti della correttezza e adeguatezza nonché degli incarichi conferiti. Qualora fosse smarrito o rubato uno di tali supporti, il possessore (di seguito Soggetto coinvolto) è tenuto a farne immediata denuncia mediante e-mail indirizzata all'Amministratore Delegato, il quale è tenuto ad avviare immediatamente idonea procedura per consentire il blocco dell'accesso a tale presidio da parte di terzi e l'eventuale cancellazione del contenuto, ove possibile. Inoltre, il Soggetto coinvolto è tenuto a denunciare presso le competenti autorità l'avvenuto smarrimento o il furto.

Il Presidente verifica gli adempimenti indicati. In caso di violazioni, il Presidente informa tempestivamente l'Organismo di Vigilanza.

Documenti di riferimento:

- Regolamento per la tutela delle informazioni riservate e il corretto utilizzo degli strumenti informatici di TIP
- Regolamento per l'attribuzione di pc aziendale
- Regolamento per l'attribuzione di telefono aziendale e sim
- Codice Etico dipendenti e collaboratori

- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo al medesimo o al Presidente.

12.21 Gestione delle licenze relative ai programmi, applicativi e software in uso

- ✓ **Potere decisionale:** Amministratore Delegato
- ✓ **Potere di gestione:** Società informatica esterna
- ✓ **Potere di controllo:** Presidente e Organismo di Vigilanza

Scopo: il presente protocollo ha lo scopo di definire le modalità di acquisto e noleggio di prodotti industriali e opere di ingegno da parte di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati in materia di violazione del diritto d'autore, previsti dall'art. 25^{novies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 171^{bis}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171^{septies}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
 - Art. 171^{octies}, L. n. 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Regolamentazione: il processo in oggetto trova specifica regolamentazione. Si identificano le seguenti macrofasi:

1. Identificazione della necessità di acquisto di programmi, applicativi e software;
 2. Controlli in ordine al venditore;
 3. Acquisto;
 4. Verifiche.
1. L'Amministratore Delegato identifica eventuali programmi, applicativi e software di rilevanza per le attività aziendali da acquistare ed informa in merito il Presidente. Si segnala, in caso di importazioni dall'estero ed esportazioni all'estero, di rispettare le procedure doganali previste dalla legge.
 2. L'Amministratore Delegato svolge le verifiche preliminari sull'affidabilità della controparte contrattuale in merito ai prodotti industriali o opere di ingegno originali e supportate da specifiche licenze che ne consentano l'utilizzo legale. Si richiede pertanto una attestazione in tal senso.
 3. In caso di esito positivo dei controlli, l'Amministratore Delegato approva l'acquisto o il noleggio e dà mandato per l'acquisto alla società informatica esterna, specificando l'obbligo di richiesta di

certificazioni attestanti l'originalità del prodotto e della licenza. L'Amministratore Delegato verifica la correttezza delle certificazioni; eventualmente richiede integrazioni o gestisce problematiche relative e può anche disporre resi.

4. Il Presidente svolge i controlli sulla correttezza delle procedure, sulla rispondenza del rapporto contrattuale con le esigenze evidenziate, sull'esecuzione delle previsioni contrattuali anche con riferimento alla consegna delle licenze. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, il Presidente informa sia l'Organismo di Vigilanza.

Documenti di riferimento:

- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo al medesimo ed al Presidente.

12.22 Gestione dei rapporti con il Collegio Sindacale e con la Società di revisione

- ✓ **Potere decisionale: Amministratore Delegato e Dirigente Preposto**
- ✓ **Potere di gestione: Assistente alla Direzione e CFO**
- ✓ **Potere di controllo: Presidente**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione dei rapporti di TIP con il Collegio Sindacale e con la Società di revisione al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ **i reati di criminalità organizzata** previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ **i reati societari** previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2621 c.c., False comunicazioni sociali
 - Art. 2621^{bis} c.c., Fatti di lieve entità
 - Art. 2622 c.c., False comunicazioni sociali delle società quotate
 - Art. 2625 c.c., Impedito controllo
 - Art. 2635 c.c., Corruzione tra privati
 - Art. 2635^{bis} c.c., Istigazione alla corruzione tra privati

Regolamentazione L'Assistente alla Direzione ed il CFO assistono il Collegio Sindacale e la Società di revisione durante le verifiche periodiche, fornendo la documentazione richiesta per le attività di propria competenza. Le richieste e le trasmissioni di dati, informazioni e ogni rilievo, comunicazione o

valutazione espresso dal Collegio Sindacale e dalla Società di revisione sono documentate e conservate a cura dell'Amministratore Delegato.

Il Presidente verifica che tutto avvenga in conformità con le procedure previste.

Documenti di riferimento:

- Codice Etico
- Regolamento interno del Collegio Sindacale

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione tra i soggetti coinvolti, anche via e-mail, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo al medesimo o al Presidente.

12.23 Gestione delle situazioni di conflitto di interesse degli Amministratori

- ✓ **Potere decisionale: Consiglio di Amministrazione**
- ✓ **Potere di gestione: Amministratore Delegato**
- ✓ **Potere di controllo: Collegio Sindacale e Organismo di Vigilanza**

Scopo: il presente protocollo ha lo scopo di definire le modalità di gestione delle situazioni di conflitto di interesse degli Amministratori di TIP al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ **i reati di criminalità organizzata** previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)
 - Art. 416^{ter} c.p., Scambio elettorale politico-mafioso
- ❖ **i reati di concussione, induzione indebita a dare o promettere utilità e corruzione** previsti dall'art. 25 del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 318 c.p., Corruzione per l'esercizio della funzione
 - Art. 319 c.p., Corruzione per un atto contrario ai doveri d'ufficio
 - Art. 319^{bis} c.p., Circostanze aggravanti
 - Art. 320 c.p., Corruzione di persona incaricata di un pubblico servizio
 - Art. 321 c.p., Pene per il corruttore
 - Art. 322 c.p., Istigazione alla corruzione
 - Art. 322^{bis} c.p., Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- ❖ **i reati societari** previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2636 c.c., Illecita influenza sull'assemblea
 - Art. 2629^{bis} c.c., Omessa comunicazione del conflitto d'interessi
 - Art. 2635 c.c., Corruzione tra privati

– Art. 2635**bis** c.c., Istigazione alla corruzione tra privati

Regolamentazione: il processo in esame si suddivide in macrofasi:

1. Individuazione delle situazioni di conflitto di interessi;
 2. Gestione delle situazioni di conflitto di interessi;
 3. Verifiche.
1. Ciascun amministratore è tenuto a informare il Consiglio di Amministrazione e l'Organismo di Vigilanza dell'insorgere di una situazione di potenziale conflitto di interesse. L'Amministratore Delegato, su richiesta del Consiglio di Amministrazione, raccoglie tutte le informazioni relative alle cariche assunte, alle partecipazioni in altre imprese o società di cui è titolare ciascun amministratore, nonché le cessazioni e le modifiche delle stesse, che possano far emergere possibili conflitti di interesse.
 2. Gli amministratori che sono portatori di determinati interessi ex art. 2391 c.c. devono darne notizia agli altri amministratori ed al Collegio Sindacale, dopo aver essere stati informati dell'operazione di TIP in relazione alla quale vi è anche il loro interesse (proprio o di terzi). Nella comunicazione devono essere indicati: (i) la natura, (ii) i termini, (iii) l'origine e (iv) la portata. Qualora tale interesse coinvolga l'Amministratore Delegato, quest'ultimo ha, in aggiunta a quanto precede, l'obbligo di astenersi dal compiere l'operazione, chiedendo al Presidente di sottoporre al Consiglio di Amministrazione la decisione in merito all'operazione. In tale ipotesi: a) dal verbale del Consiglio di Amministrazione devono emergere le ragioni e la convenienza per la Società dell'operazione; b) l'Amministratore Delegato si astiene nella votazione. Qualora l'operazione sia qualificabile come "operazione con parti correlate" – ai sensi dell'art. 2391-*bis* c.c., Regolamento Consob Operazioni con Parti Correlate e della Procedura interna dell'ente – trovano applicazione le corrispondenti discipline della Procedura e del Regolamento organizzativo del Comitato Controllo e Rischi e Parti Correlate. Viceversa, l'amministratore che versa in una situazione di conflitto di interesse è tenuto ad astenersi dalla decisione qualora il conflitto di interesse sia limitato ad essa. Tuttavia, se il conflitto di interesse è connesso all'intera attività all'interno del Consiglio di Amministrazione, l'amministratore, se il Consiglio non ritiene di soprassedere sulla incompatibilità, dà le proprie dimissioni, secondo le procedure aziendali e statutarie.
 3. Il Collegio Sindacale svolge i controlli sulla correttezza delle procedure, sulla rispondenza del rapporto contrattuale con le esigenze evidenziate sull'esecuzione delle previsioni contrattuali. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, informa l'Organismo di Vigilanza.

Documenti di riferimento:

- Procedura - *Risk Client Evaluation*
- Codice Etico - Conflitti di interesse
- Procedure per le operazioni con Parti Correlate

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione, anche via email, per l'archiviazione della relativa documentazione. Tutta la documentazione è conservata a cura dell'Amministratore Delegato, che la custodisce in apposito armadio chiuso ovvero, se telematica, è accessibile mediante credenziali note solo allo stesso.

12.24 Gestione dei prodotti e rifiuti, compilazione dei registri di controllo e flussi informativi verso le Autorità di Vigilanza

- ✓ **Potere decisionale: Amministratore delegato**
- ✓ **Potere di gestione: Addetto dell'Ufficio di Segreteria e personale di Area competente, con il supporto di ditte esterne autorizzate allo smaltimento dei rifiuti**
- ✓ **Potere di controllo: Organismo di Vigilanza e Consiglio di Amministrazione**

Scopo: il presente protocollo ha lo scopo di definire le modalità adottate da TIP per la corretta gestione dei rifiuti aziendali prodotti durante lo svolgimento delle attività lavorative al fine di prevenire la commissione dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. n. 231/2001.

In particolare, con questo protocollo si vogliono prevenire:

- ❖ i reati di criminalità organizzata previsti dall'art. 24^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 416 c.p., Associazione per delinquere (anche transnazionale)
 - Art. 416^{bis} c.p., Associazioni di tipo mafioso anche straniere (anche transnazionale)
- ❖ i reati societari previsti dall'art. 25^{ter} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 2635 c.c., Corruzione tra privati
 - Art. 2635^{bis} c.c., Istigazione alla corruzione tra privati
- ❖ i reati ambientali previsti dall'art. 25^{undecies} del Decreto, ovvero le fattispecie, consumate o tentate, di:
 - Art. 256, D.lgs. n. 152/2006, Attività di gestione di rifiuti non autorizzata
 - Art. 258, D.lgs. n. 152/2006, Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari
 - Art. 259, D.lgs. n. 152/2006, Traffico illecito di rifiuti
 - Art. 260, D.lgs. n. 152/2006, Attività organizzate per il traffico illecito di rifiuti.
 - Art. 260^{bis}, D.lgs. n. 152/2006, Sistema informatico di controllo della tracciabilità dei rifiuti.

Regolamentazione: il processo in esame si suddivide in macrofasi:

1. Individuazione degli adempimenti in relazione alla gestione dei prodotti, sottoprodotti e rifiuti;
 2. Gestione degli adempimenti relativi, ivi compresa la compilazione dei registri;
 3. Verifiche.
1. Qualora siano previste particolari modalità di gestione dei prodotti, sottoprodotti, rifiuti, l'Addetto all'Ufficio di Segreteria informa l'Amministratore Delegato. L'Addetto all'Ufficio di Segreteria, anche avvalendosi del supporto di ditte esterne autorizzate allo smaltimento dei rifiuti, viene a conoscenza di tutti gli adempimenti necessari e ne informa il personale di Area competente al fine di eseguirli.
 2. Il personale di Area competente esegue le indicazioni fornite dalla ditta esterna. Qualora necessario, il Responsabile di Area competente gestisce i flussi informativi verso le Autorità di Vigilanza, salvo che sia necessaria la partecipazione diretta dell'Amministratore Delegato. In caso di difformità o problematiche di sorta, il Responsabile di Area competente sottopone la questione

all'Amministratore Delegato, che effettua le valutazioni del caso e decide come procedere.

3. L'Amministratore Delegato svolge i controlli sulla correttezza delle procedure e sulla rispondenza degli adempimenti con le previsioni di legge evidenziate. In caso ravvisi violazioni nelle procedure o aree di rischio di reato, l'Amministratore Delegato informa sia l'Organismo di Vigilanza sia il Consiglio di Amministrazione.

Documenti di riferimento:

- Procedura - Rifiuti Aziendali
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: tutte le fasi del processo sono opportunamente documentate e oggetto di comunicazione, anche via e-mail, per l'archiviazione della relativa documentazione. L'Addetto all'Ufficio di Segreteria cura l'archiviazione della documentazione, che deve avvenire in armadio chiuso dotato di serratura ovvero, se su supporto telematico, attraverso un accesso chiuso. Le chiavi e gli identificativi sono a disposizione solo dell'Amministratore Delegato e del Consiglio di Amministrazione. In caso di assenza di evidenza documentale, è predisposta verbalizzazione di quanto accaduto dall'Addetto all'Ufficio di Segreteria, sottoscritta per l'approvazione dell'Amministratore Delegato.

12.25 Le attività d'ufficio

- ✓ **Potere decisionale:** Datore di Lavoro ai sensi dell'art. 2 lett. b) D. Lgs. 81/2008;
- ✓ **Potere di gestione:** Lavoratore ai sensi dell'art. 2 lett. a) D. Lgs. 81/2008;
- ✓ **Potere di controllo:** RSPP per l'aspetto tecnico, RLS e Preposti ai sensi dell'art. 2 lett. e) D. Lgs. 81/2008

Regolamentazione: il processo si articola in macrofasi per l'area omogenea che nel seguito e per comodità viene indicata con il termine "ufficio":

- Individuazione delle attività di rischio;
- Gestione del rischio;
- Diffusione delle procedure ed estratto del DVR;
- Controllo del rispetto delle procedure;
- Azioni correttive – piani di miglioramento;
- Verifiche.

1. Ciascun Lavoratore identifica eventuali ulteriori rischi, ove non previsti, connessi alla propria attività e riferisce al Datore di Lavoro o RLS nei casi previsti dal Testo Unico;
2. Il Datore di Lavoro, tenuto conto delle informative ricevute, da indicazioni al RSPP al fine di valutare il rischio emerso sotto il profilo meramente tecnico. Il medesimo RSPP, nei limiti della rispettiva competenza, identifica eventuali procedure atte a evitare il rischio ovvero, ove non evitabile, a circoscriverlo e a prevedere apposite misure, condividendo le proprie attività con il Datore di Lavoro, che ne verifica l'adeguatezza. Il Datore di Lavoro deve dare sempre l'assenso ovvero suggerire revisioni.

3. Il Datore di Lavoro si impegna a divulgare tra i Lavoratori le procedure, eventualmente adottate organizzando e gestendo appositi programmi di informazione, formazione ed il corretto recepimento degli stessi, anche per il tramite dei Preposti e, se del caso, coinvolgendo il RSPP.
4. I Preposti verificano il rispetto delle procedure e, qualora ravvisino inadeguatezze delle stesse, informano il Datore di Lavoro.
5. I Preposti, il RLS ed il RSPP, per i soli aspetti tecnici, svolgono i controlli sulla correttezza delle procedure e sulla rispondenza delle stesse con le esigenze evidenziate e con le mansioni spettanti ai soggetti coinvolti. In caso ravvisino violazioni nelle procedure, violazioni di legge o pericoli di commissione di reati, informano il Datore di Lavoro. Nel caso in cui il Datore di Lavoro ravvisi autonomamente violazioni perpetrate nelle procedure, violazioni di legge o pericoli di commissione di reati, informa l'OdV.

Documenti di riferimento:

- Documento di Valutazione dei Rischi (DVR)
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: Il Datore di Lavoro cura l'archiviazione della documentazione, che deve avvenire in armadio chiuso dotato di serratura ovvero, se su supporto telematico, attraverso un accesso riservato.

12.26 I rapporti con i soggetti esterni ai sensi dell'art. 26 del D.Lgs. n. 81/2008 (in particolare, affidamento dei lavori all'impresa appaltatrice o a lavoratori autonomi all'interno dell'Ente)

- ✓ **Potere decisionale: Datore di Lavoro ai sensi dell'art. 2 lett. b) D. Lgs. 81/2008;**
- ✓ **Potere di gestione: Lavoratore ai sensi dell'art. 2 lett. a) D. Lgs. 81/2008;**
- ✓ **Potere di controllo: RSPP per l'aspetto tecnico e Preposti ai sensi dell'art. 2 lett. e) D. Lgs. 81/2008;**

Regolamentazione: il presente processo si distingue in macrofasi:

- Individuazione del rapporto e pre-qualifica dei requisiti tecnico professionali;
- Individuazione dei rischi interferenziali;
- Adempimenti e misure adottate;
- Verifiche.

1. Nell'ipotesi in cui sia necessario affidare dei lavori ad un'impresa appaltatrice o avvalersi di lavoratori autonomi chiamati ad operare all'interno della società, ai sensi dell'art. 26 del D. Lgs. 81/2008, il Datore di Lavoro, verifica, preventivamente, l'idoneità tecnico professionale degli stessi, acquisendo, ove ritenuto opportuno, documentazione quale, a titolo meramente esemplificativo, copia del certificato di iscrizione alla Camera di Commercio, industria, artigianato, ovvero DURC, elenco attrezzature, attestati formazione, fornitura DPI, ovvero autocertificazioni (in caso residuale di emergenza), attuando tutti gli adempimenti previsti dalla normativa.

2. Conclusa la fase di pre-qualifica, l'Amministratore Delegato, anche avvalendosi dell'ausilio della figura tecnica espressamente individuata dalla Azienda (RSPP), riscontra i rischi interferenziali e le soluzioni da adottare per l'eliminazione ovvero riduzione degli stessi.

3. L'Amministratore Delegato organizza, solo nel caso in cui la fornitura abbia oggettivi profili di rischio rilevante, la riunione di coordinamento con i fornitori coinvolti nella attività. Durante tale riunione viene condiviso il DUVRI, riportando nel corpo del medesimo i rischi interferenziali e le misure adottate. Tale documento deve essere firmato dai Preposti competenti e dai Responsabili identificati dalle Società appaltatrici. L'Amministratore Delegato verifica che il DUVRI divenga allegato imprescindibile al contratto e/o all'ordine commerciale.

4. I Preposti, ed il RSPP per le questioni tecniche, svolgono i controlli sulla correttezza delle procedure e sulla rispondenza delle stesse con le esigenze evidenziate e con le mansioni spettanti ai soggetti coinvolti. Qualora ravvisino violazioni nelle procedure, violazioni di legge o pericoli di commissione di reati, informano, anche disgiuntamente, il Datore di Lavoro.

Documenti di riferimento:

- Documento di Valutazione dei Rischi (DVR)
- Procedura per l'affidamento lavoro in appalto
- Codice Etico
- Codice Etico dipendenti e collaboratori
- Codice Etico Informatico

Tracciabilità: Il Datore di Lavoro, ai sensi del D. Lgs. 81/2008, cura l'archiviazione della documentazione, che deve avvenire in armadio chiuso dotato di serratura ovvero, se su supporto telematico, attraverso un accesso riservato.