MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Ex D. Lgs. 231/2001

Aggiornato con delibera del Consiglio di Amministrazione nella riunione del 08 Novembre 2012

1^ ed.) Approvato dal Consiglio di Amministrazione di Data Service S.p.A. nella seduta del 10.09. 2004.

2^ed.) Aggiornato ed approvato dal Consiglio di Amministrazione di B.E.E. TEAM S.p.A. nella seduta del 13.11.2009.

3^ed.) Aggiornato in data 25.02.2011 e successivamente nella seduta del 25.03.2011 approvato dal Consiglio di Amministrazione di B.E.E. TEAM S.p.a.

4^ ed.) Aggiornato in data 02.05.2011 a seguito della delibera, assunta il 28.04.2011, dall'Assemblea degli Azionisti di B.E.E. TEAM S.p.a.

5^ ed.) Aggiornato ed approvato dal Consiglio di Amministrazione di B.E.E. TEAM S.p.A. nella seduta del 28.07.2011.

6^ ed.) Aggiornato ed approvato dal Consiglio di Amministrazione di B.E.E. TEAM S.p.A. nella seduta del 10.11.2011.

7^ ed.) Aggiornato ed approvato dal Consiglio di Amministrazione di B.E.E. TEAM S.p.A. nella seduta del 08.11.2012

INDICE

PARTE GENERALE:

PREMESSA 8

1. IL DECRETO LEGISLATIVO n. 231/2001 9

Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società ed associazioni 9

2. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO 16

2.1 Struttura del Modello 16
2.2 Destinatari del Modello 17
2.3 Reati presupposto per i quali si stima vi sia un rischio di reato: elencazione delle fattispecie 17
2.4 Reati presupposto per i quali, in relazione all'attività svolta dalla Società e al suo contesto operativo, non si stima ipotizzabile un rischio di commissione ma su cui verrà comunque effettuata un'attività di vigilanza; elencazione delle fattispecie 19
2.5 Approvazione e recepimento dei principi di riferimento del Modello 21

3. ORGANISMO DI VIGILANZA 21

3.1 Identificazione dell'Organismo di Vigilanza 21
3.2 Regolamento sulle modalità di nomina, cessazione e sostituzione dei componenti dell'Organismo di Vigilanza 22
3.3 Funzioni e poteri dell'Organismo di Vigilanza 23
3.4 Reporting dell'Organismo di Vigilanza nei confronti degli organi societari 24

4. OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA 25

4.1 Raccolta e conservazione delle informazioni 26

5. FORMAZIONE E COMUNICAZIONE 26

6. SISTEMA DISCIPLINARE 27

6.1 Funzione del sistema disciplinare 27
6.2 Il sistema disciplinare 27
6.3 Soggetti titolati a comminare i provvedimenti disciplinari 30

7. MODELLO E CODICE ETICO 30

PARTE SPECIALE "A":

(REATI IN DANNO DELLA PUBBLICA AMMINISTRAZIONE EX ART. 24 E 25 DEL D. LGS. 231/2001)

FUNZIONE DELLA PARTE SPECIALE 33

B.E.E. Team spa –Tutti i diritti riservati.

TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE 33

RESPONSABILI INTERNI E SCHEDE DI EVIDENZA 33
POTENZIALI AREE A RISCHIO E REGOLE DI COMPORTAMENTO 34
PROCESSI OPERATIVI:
- GESTIONE VERIFICHE ED ISPEZIONI 36
- OBBLIGHI PREVIDENZIALI 38

PROCESSI STRUMENTALI:
- SELEZIONE DEL PERSONALE 40
- FINANZA DISPOSITIVA E TESORERIA..... 42
- CONSULENZE 44
- GESTIONE CONTENZIOSO E PRECONTENZIOSO..... 46
- ACQUISTO DI BENI E SERVIZI 48

PARTE SPECIALE "B":
(REATI SOCIETARI EX ART 25 TER E SEXIES D. LGS. 231/2001)

FUNZIONE DELLA PARTE SPECIALE..... 51
TIPOLOGIA DEI REATI SOCIETARI E DI MARKET ABUSE..... 51
PROCESSI SENSIBILI NELL'AMBITO DEI REATI SOCIETARI E DI M.A..... 51
DESTINATARI DELLA PARTE SPECIALE 51
REGOLE GENERALI 52
DOCUMENTI DIFFUSI TRA GLI ORGANI SOCIALI DI B.E.E. TEAM SPA ... .55
PROCEDURE E CONTROLLI SPECIFICI 65
FLUSSI VERSO L'ORGANISMO DI VIGILANZA 66

PARTE SPECIALE "C":
(REATI DI OMICIDIO COLPOSO E DI LESIONI COLPOSE GRAVI E GRAVISSIME IN VIOLAZIONE DEGLI ADEMPIENTI IN MATERIA DI TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LAVORO EX ART. 25 SEPTIES D. LGS. 231/01)

FUNZIONI DELLA PARTE SPECIALE 69
REGOLE GENERALI 69
PROCEDURE SPECIFICHE 80

PARTE SPECIALE "D":
(REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO BENI O UTILITA' DI PROVENIENZA ILLECITA EX ART. 25 OCTIES D. LGS. 231/01)

PREMESSA 82
PROCESSI SENSIBILI..... 82
REGOLE GENERALI 83
PROCEDURE SPECIFICHE 85

PARTE SPECIALE "E":
(AREE DI ATTIVITA' NEL CUI AMBITO POSSONO ESSERE COMMESSI I REATI INFORMATICI PREVISTI DALL'ARTICOLO 24 BIS DEL D. LGS. 231/01 (INTRODOTTO DALLA LEGGE 48/2008)

PREMESSA 86

B.E.E. Team spa –Tutti i diritti riservati.

FUNZIONE DELLA PARTE SPECIALE..... 86
DESTINATARI DELLA PARTE SPECIALE..... 89
PROCESSI SENSIBILI 90
REGOLE GENERALI 92
ATTIVITÀ DELL'ORGANISMO DI VIGILANZA 97
FLUSSI VERSO L'ORGANISMO DI VIGILANZA 97
PROCEDURE SPECIFICHE 97

PARTE SPECIALE "F"
REATI DI CRIMINALITÀ ORGANIZZATA PREVISTI DALL'ARTICOLO 24 *TER* DEL D.LGS. 231/01 (INTRODOTTO DALLA L. 15 LUGLIO 2009, N. 94, ART. 2, CO. 29) E REATI TRANSNAZIONALI (DI CUI ALL'ART. 10 DELLA LEGGE 26/03/2006, N. 146)

PREMESSA..... 100
FUNZIONE DELLA PARTE SPECIALE..... 102
DESTINATARI DELLA PARTE SPECIALE..... 102
PROCESSI SENSIBILI..... 102
REGOLE GENERALI..... 103
PROCEDURE SPECIFICHE..... 107

PARTE SPECIALE "G"
REATI DI ABBANDONO E DEPOSITO INCONTROLLATO DI RIFIUTI SUL SUOLO E NEL SUOLO (INTRODOTTI CON D.LGS. 152/2006)

PREMESSA..... 109
FUNZIONE DELLA PARTE SPECIALE..... 111
DESTINATARI DELLA PARTE SPECIALE..... 112
PROCESSI SENSIBILI..... 113
REGOLE GENERALI..... 113
PROCEDURE SPECIFICHE..... 114

APPENDICE
A. OPERAZIONI PROMANATE DIRETTAMENTE E "FUORI PROCEDURA" DAI SOGGETTI APICALI..... 115
B. PRINCIPI GENERALI DI CONTROLLO INTERNO 116
C. PRINCIPI DI COMPORTAMENTO CON LA PUBBLICA AMMINISTRAZIONE 117
D. SOGGETTI PUBBLICI INTERFACCIABILI AI SENSI DGLS 231/2001..... 120

ALLEGATO 1
SCHEDA DI EVIDENZA – RISCHIO REATI V/ LE PP.AA..... 121

ALLEGATO 2
FLUSSI VERSO L'ORGANISMO DI VIGILANZA 122

ALLEGATO 3
RISCHI RESIDUI..... 135

B.E.E. Team spa –Tutti i diritti riservati.

PARTE GENERALE

B.E.E. Team spa –*Tutti i diritti riservati.*

PREMESSA

B.E.E. TEAM Spa intende allinearsi ai comportamenti etici al fine di assicurare sempre maggiori condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali.

Con questo documento B.E.E. TEAM Spa, anche alla luce del chiarimento espresso nelle Linee Guida di Confindustria qui di seguito riportate, intende dotarsi di un "Modello di organizzazione, gestione e controllo" ex Decreto Legislativo 231/01 con caratteristiche di snellezza e flessibilità in quanto orientato ad una "piccola impresa",:

" ... *Una piccola impresa, la cui definizione va ricercata più che in parametri quantitativi, nella essenzialità della struttura interna gerarchica e funzionale* ... "

Ciò premesso si è proceduto all'adattamento dello stesso alla realtà di B.E.E. TEAM Spa, fondandolo sulla specifica individuazione dei processi nel cui ambito possono essere commessi i reati (Risk analysis sui processi/attività aziendali).

Le fondamentali attività svolte per rispondere ai dettami del D. Lgs. in argomento sono:

1. **INDIVIDUAZIONE DEI RISCHI:** analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D. Lgs. n. 231/2001. I rischi evidenziati sono stati valutati nelle analisi svolte tenendo conto di due parametri fondamentali:
    - la probabilità di accadimento dell'evento negativo;
    - la severità di impatto dello stesso.

    I suddetti parametri sono stati utilizzati per identificare una scala di priorità dei provvedimenti preventivi da mettere in campo per fronteggiare le possibili problematicità, per impostare le regole generali di comportamento operativo cui devono attenersi i dipendenti ed i terzi della Società nelle fattispecie a rischio identificate (regole riportate nelle "parti speciali" A e B del presente Modello Organizzativo) e per dare corpo operativo all'aggiornamento del quadro dispositivo aziendale. Circa i valori dei "rischi residui" risultanti dai test realizzati nel mese di luglio 2011 vedasi allegato 3.

2. **PROGETTAZIONE DEL SISTEMA DI PROTOCOLLI:** valutazione del sistema di controllo esistente all'interno della società ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi identificati

3. **CODICE ETICO E SISTEMA DISCIPLINARE:** adozione del Codice Etico della società controllante, adattato alle specificità della realtà aziendale ed all'intero Gruppo.

4. **ORGANISMO DI VIGILANZA:** nomina di un proprio Organismo di Vigilanza.

1. IL DECRETO LEGISLATIVO n. 231/2001

Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni

Il Decreto, recante "*disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", ha introdotto nell'ordinamento giuridico italiano alcune sostanziali novità:

- un regime di **responsabilità amministrativa** (assimilabile alla responsabilità penale) a carico degli Enti (società, associazioni, consorzi,…): per *reati nei confronti della Pubblica Amministrazione* (art. 24 e 25 del Decreto), quelli *contro il patrimonio commessi a danno dello Stato o di altro ente pubblico* (art. 25-*bis* del Decreto), per i *reati societari* elencati nell'art. 25-*ter,* per i *delitti* (di cui all'art. 25-*quater) aventi finalità di terrorismo o di eversione dell'ordine democratico*, nonché dei *delitti che siano comunque stati posti in essere in violazione di quanto previsto dall'art. 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo* fatta a New York il 9 dicembre 1999, (tassativamente elencati ed identificati). Per completezza di informativa, si segnala che da ultimo è stato inserito l'art. 25-*quinques* che estende il regime della responsabilità amministrativa dell'ente anche in relazione alla commissione dei delitti contro la personalità individuale come descritti nella legge 228/03 contenente "misure contro la tratta delle persone".
  Le Leggi 62/2005 e 262/2005 hanno ulteriormente ampliato la tipologia di reati la cui commissione può comportare la responsabilità amministrativa degli enti: in particolare, la prima ha introdotto l'art. 25-*sexies*, che prevede la punibilità dell'Ente nel cui interesse o vantaggio siano stati commessi i c.d reati di "*market abuse" (abuso di informazioni privilegiate e manipolazione del mercato)* mentre la seconda, oltre ad alcune modifiche introdotte in tema di reati societari, ha esteso l'applicabilità del Decreto 231/2001 al reato di omessa comunicazione del conflitto di interessi.
  L'art. 25-*septies* (introdotto dalla l. 123/2007 e confermato dal D. Lgs. 81/2008) ha poi esteso la responsabilità amministrativa dell'ente ai reati di omicidio e lesioni colpose gravi o gravissime (artt. 589-590 c.p.), commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, mentre analoga estensione è prevista dall'art. 25-octies (inserito dal D. Lgs. 231/2007) per i reati di ricettazione (art. 648), riciclaggio (art. 648 bis) e impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter). I reati di riciclaggio e d'impiego di denaro, beni o utilità di provenienza illecita erano già rilevanti ai fini del D. Lgs. 231/01, ma esclusivamente se transnazionali (ex art. 10 L. 146/06). A seguito dell'introduzione dell'art. 25-octies, i predetti reati – unitamente alla ricettazione – divengono rilevanti anche su base nazionale.

Generano altresì responsabilità dell'ente i reati transnazionali[1] disciplinati dalla l. 146/2006: qualora commessi nelle condizioni indicate in nota, vengono in considerazione le seguenti fattispecie: induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.); favoreggiamento personale (art. 378 c.p.); associazione per delinquere (art. 416 c.p.); associazione di tipo mafioso (art.416-bis c.p.); associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater d.P.R. 43/73); associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 d.P.R. 390/1990); traffico di migranti (art.12, comma 3, 3-bis, 3-ter e 5 TU D. Lgs.. 25 luglio 1998 n.286).

Con la l. 48/2008 è stato introdotto nel D. Lgs. 231/01 l'art. 24 bis, che inserisce fra i reati presupposto una serie di reati informatici, e in particolare: falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491-bis c.p.); accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.); detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.); diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.); intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.); installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.); danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.); danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.); danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.); danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.); frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.) .

Sono stati poi introdotti nel novero dei delitti previsti dal D. Lgs. 231/01:

- delitti contro l'industria e il commercio (art. 25-bis.1., D. Lgs. 231/01, aggiunto dalla legge n. 99 del 23/07/09), ossia Turbata libertà dell'industria o del commercio (art. 513 c.p.); - frode nell'esercizio del commercio (art. 515 c.p.); - vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.); - vendita di prodotti industriali con segni mendaci (art. 517 c.p.); - fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.); - contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.); - illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.); - frodi contro le industrie nazionali (art. 514);

1 Si considera "reato transnazionale" il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

- delitti di criminalità organizzata (art. 24-ter, D. Lgs. 231/01, aggiunto dalla legge n. 94 del 15 luglio 2009, art. 2, co. 29) ossia: associazione a delinquere (art. 416 c.p. - con un regime sanzionatorio più grave quando finalizzata alla riduzione o mantenimento in schiavitù o in servitù, alla tratta di persone o all'acquisto e alienazione di schiavi, ai sensi del comma sesto); associazioni di tipo mafioso (art. 416 bis c.p.) e delitti commessi per agevolare tali associazioni (art. 7 legge 203/91); sequestro di persona a scopo di rapina o di estorsione (art. 629 c.p.); associazione a delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 d.p.r. 309/90);

- delitti in materia di violazione del diritto d'autore (art. 25-novies, D. Lgs. 231/01 aggiunto dalla legge n. 99 del 23/07/09) - messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis); - reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3) - abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1); - riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2); - abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941); - mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941); - fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies l. 633/1941).

- delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-novies, D. Lgs. 231/01 aggiunto dalla L. 3 agosto 2009 n. 116, art. 4) - Induzione

a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.), figura questa già prevista dalla legge 146/06 sulla criminalità transazionale, ma solo nel caso in cui si configurasse come tale.

- La natura della responsabilità dell'Ente

La responsabilità dell'ente **è una responsabilità autonoma** rispetto a quella delle persone fisiche che hanno commesso i reati indicati nell'elenco del D. Lgs. 231/01 (a detti reati vanno aggiunti, in quanto generatori di responsabilità dell'ente, gli illeciti amministrativi in materia di market abuse di cui agli artt. 187 bis e 187 ter D. Lgs. 58/98).

La responsabilità dell'ente dipende da due distinti criteri di ascrizione: sul piano oggettivo occorre, da un lato, che il reato (o l'illecito amministrativo) c.d. presupposto[2] sia stato realizzato a vantaggio o nell'interesse dell'ente stesso (in altri termini che l'ente abbia tratto un beneficio dalla commissione dell'illecito ovvero che nel porre in essere la condotta vietata da parte dell'agente fosse prospettabile il prodursi di un beneficio a favore dell'ente medesimo); dall'altro – sempre sul piano oggettivo – occorre che il fatto illecito sia stato realizzato da un soggetto che rivesta funzioni di rappresentanza, di amministrazione o di direzione all'interno dell'ente (c.d. soggetti apicali), ovvero da un soggetto sottoposto alla direzione o alla vigilanza di un soggetto in posizione apicale.

Sul piano soggettivo occorre poi che all'ente sia attribuibile una colpa per inadeguata organizzazione, che il sistema normativo modula in modo diverso a seconda che il reato presupposto sia posto in essere da un soggetto in posizione apicale ovvero da un soggetto sottoposto alla direzione, vigilanza o controllo di un 'apicale'.

Prima di esaminare le differenze cui si è fatto cenno, è decisivo riconoscere che la misura della colpa nell'organizzazione – che fonda la responsabilità dell'ente – trova il proprio metro nella adozione e nel costante aggiornamento di un modello di organizzazione, gestione e controllo efficace ed efficiente, idoneo cioè a prevenire reati della specie di quelli c.d. reati-presupposto.

- Se il fatto illecito è commesso da un soggetto in posizione subordinata, la responsabilità dell'ente non sussiste se l'illecito stesso «è stato reso possibile dall'inosservanza degli obblighi di direzione o vigilanza» e comunque la responsabilità è esclusa se, prima della commissione del reato, è stato **«adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi» (art. 7 D. Lgs. 231/01).**

Se il fatto illecito è stato posto in essere da un soggetto in posizione apicale, l'onere della prova viene addossato all'ente, che deve quindi dimostrare che la preesistenza al fatto di un modello organizzativo efficiente ed efficace, tale che il reato è stato «commesso eludendo fraudolentemente i modelli organizzativi e di gestione» (art. 6 D. Lgs. 231/01).

2 I reati-presupposto sono unicamente quelli tassativamente indicati dal D. Lgs. 231/01 (oltre ai ricordati illeciti amministrativi di cui al D. Lgs. 58/98).

L'art. 6 del Decreto dispone, infine, che tali modelli possano essere adottati sulla base di codici di comportamento redatti da associazioni rappresentative di categoria. In tal senso, in data 7 marzo 2002, Confindustria ha approvato le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/01", successivamente aggiornate in seguito alle osservazioni inviate dal Ministero della Giustizia. In data 31 marzo 2008 Confindustria ha emanato una nuova edizione delle ricordate Linee Guida, aggiornate alla data medesima, approvate dal Ministero della Giustizia con comunicazione in data 2 aprile 2008. –

Il percorso indicato dalle citate Linee Guida per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

- mappatura degli ambiti aziendali di attività con individuazione delle aree a rischio;
- analisi dei rischi potenziali riguardo alle possibili modalità attuative dei reati nelle diverse aree individuate secondo il processo sopra indicato;
- valutazione/costruzione/adeguamento del sistema di controlli preventivi (protocolli) idonei a ridurre/mantenere i rischi di commissione dei reati.

Il compimento di questo percorso consente di pervenire ad un sistema di controllo in grado di ridurre i rischi attraverso l'adozione degli appositi protocolli di prevenzione individuati.

Le componenti più rilevanti del sistema di controllo preventivo proposto da Confindustria sono:

- codice etico;
- sistema organizzativo;
- procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- sistema di controllo e gestione;
- comunicazione al personale e sua formazione.

Secondo le indicazioni di Confindustria, il sistema di controllo interno deve inoltre essere uniformato ai seguenti principi generali[3]:

Sistema di Controllo Interno

E' l'insieme degli "strumenti" volti a fornire ragionevole garanzia circa il raggiungimento degli obiettivi di efficienza ed efficacia operativa, affidabilità delle informazioni finanziarie e gestionali, rispetto delle leggi e dei regolamenti, nonché salvaguardia del patrimonio anche contro possibili frodi. Il Sistema di Controllo

[3] - In riferimento al modello di controllo interno di cui al documento "Integrated Control: Integrated Framework" [1992], autorizzato dal Committee of Sponsoring Organizations of the Treadway Commission (c.d. "CoSO Report").

Interno si qualifica con principi generali il cui campo di applicazione si estende con continuità attraverso i diversi livelli organizzativi (Business Unit, Funzione, - nel seguito, indicati con unità organizzativa).

1. *Ambiente generale di controllo*

Le responsabilità devono essere definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto

Nessuna operazione significativa (in termini quali-quantitativi) per l' unità organizzativa può essere originata/attivata senza autorizzazione

I poteri di rappresentanza devono essere conferiti secondo ambiti di esercizio e limiti di importo strettamente collegati alle mansioni assegnate ed alla struttura organizzativa.

I sistemi operativi devono essere coerenti con le politiche aziendali ed il Codice Etico; in particolare, le informazioni finanziarie della Società devono essere predisposte:

- nel rispetto delle leggi e dei regolamenti,
- nel rispetto dei principi contabili statuiti
- in coerenza con le procedure amministrative definite
- nell'ambito di un completo ed aggiornato piano dei conti.

2. *Valutazione dei rischi*

Gli obiettivi dell' unità organizzativa devono essere definiti e comunicati a tutti i livelli interessati, al fine di rendere gli stessi chiari e condivisi.

Devono essere individuati i rischi connessi al raggiungimento degli obiettivi, prevedendone periodicamente il monitoraggio e l'aggiornamento

Gli eventi negativi che possono minacciare la continuità operativa devono essere oggetto di apposita attività di valutazione dei rischi e di adeguamento delle protezioni

3. *Attività di controllo*

Nessuno deve avere il pieno controllo di un intero processo/attività, ma deve essere prevista a livello procedurale un'adeguata separazione dei ruoli.

I processi operativi devono essere definiti prevedendo un adeguato supporto documentale/di sistema per consentire che siano sempre verificabili in termini di congruità, coerenza e responsabilità

Le scelte operative devono essere tracciabili in termini di caratteristiche e motivazioni e devono essere individuabili coloro che hanno autorizzato, effettuato e verificato le singole attività

Lo scambio di informazioni fra fasi/processi contigui deve prevedere meccanismi (riconciliazioni, quadrature, ecc.) per garantire l'integrità e la completezza dei dati gestiti.

4. *Informazioni e Comunicazione*

Deve essere previsto un sistema di indicatori per processo/attività ed un relativo flusso periodico di reporting verso il management

I Sistemi Informativi amministrativi e gestionali devono essere orientati all'integrazione ed alla standardizzazione.

I meccanismi di sicurezza devono garantire la protezione/accesso fisico÷logico ai dati e ai beni di ogni unità organizzativa.

B.E.E. Team spa *–Tutti i diritti riservati.*

5. *Monitoraggio*

Il sistema di controllo è soggetto ad attività di supervisione continua e di valutazione periodica finalizzate al costante adeguamento

In coerenza con i principi sopra esposti e con le specifiche previsioni del D.Lgs 231/01, il sistema di controllo deve essere caratterizzato da:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- presenza di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal modello;
- individuazione e nomina dell'Organismo di Vigilanza;
- obbligo da parte delle funzioni aziendali, e segnatamente di quelle individuate come maggiormente "a rischio", di fornire informazioni all'O.d.V., anche su base strutturata, e di segnalare anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (in quest'ultimo caso l'obbligo è esteso a tutti i dipendenti senza seguire linee gerarchiche);

Resta inteso che la scelta di non seguire in alcuni punti specifici le Linee Guida non inficia la validità di un Modello. Questo infatti, essendo redatto con riferimento alla peculiarità di una determinata società, può discostarsi dalle Linee Guida che per loro natura hanno carattere generale.

Tenendo nella dovuta considerazione il documento emesso da Confindustria, sopra sintetizzato nei suoi lineamenti essenziali, B.E.E. TEAM Spa ha deciso di adeguare il proprio Modello di organizzazione, gestione e controllo ai requisiti espressamente richiesti nel D. Lgs. 231/2001.

2. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

2.1 Struttura del Modello

Il presente Modello si compone di una parte generale e da singole parti speciali, per le diverse tipologie di reato a tutt'oggi contemplate nel Decreto, così articolate:

- Parte Speciale "A": trova applicazione per le tipologie specifiche di reati realizzabili in danno della Pubblica Amministrazione previste ai sensi degli art. 24 e 25 del D. Lgs. 231/01.
- Parte Speciale "B": si riferisce invece ai reati societari di cui all'art. 25 ter ed ai reati ed illeciti amministrativi di abuso di informazioni privilegiate e di manipolazione del mercato di cui all'art. 25 *sexies* del D. Lgs. 231/01.
- Parte Speciale "C": relativa ai Reati di omicidio colposo e di lesioni colpose gravi e gravissime in violazione degli adempienti in materia di tutela della salute e della sicurezza sul lavoro. (Art . 25 *septies* D. Lgs. 231/01).
- Parte Speciale "D": tratta i reati di riciclaggio, ricettazione impiego di denaro, beni o utilità di provenienza illecita introdotti dall'art. 63, co. 3 del D. Lgs. 231/07, nel decreto n. 231/2001 (art. 25-*octies).*
- Parte Speciale "E": in merito ai delitti informatici ed al trattamento illecito di dati, reati previsti dall'articolo 24 bis del D. Lgs. 231/01 (introdotto dalla Legge 48/2008).
- Parte Speciale "F": in materia di reati di criminalità organizzata previsti dall'articolo 24 ter del D.Lgs. 231/01 (introdotto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29) e reati transnazionali (di cui all'art. 10 della Legge 26/03/2006, n. 146).
- Parte Speciale "G": in materia di reati di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo (introdotti con d.lgs. 152/2006).

Inoltre, costituisce parte integrante del Modello il Codice Etico, nel quale sono espressi i principi generali ed i valori cui deve essere ispirata l'attività di tutti coloro che a qualsiasi titolo operano per conto di B.E.E. Team. spa. Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma dalla Società ed è suscettibile di applicazione sul piano generale da parte della Società allo scopo di esprimere i principi di "deontologia aziendale" che B.E.E. Team. spa. riconosce come propri e all'osservanza dei quali richiama tutti gli Esponenti Aziendali;
- il Modello, declinando in concreto i principi contenuti nel Codice Etico, risponde alle specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati o di illeciti amministrativi, nonché condotte o comportamenti ad essi prodromici.

E' stato affidato dall'Assemblea degli Azionisti in data 29 aprile 2011 ad un organismo della Società dotato di autonomi poteri di iniziativa e di controllo, denominato Organismo di Vigilanza (v. oltre Capitolo 3), il compito di vigilare sul funzionamento e sull'osservanza del Modello, nonché di proporne l' aggiornamento.

2.2 Destinatari del Modello

Si considerano Destinatari del presente Modello e, come tali e nell'ambito delle specifiche competenze, tenuti alla sua conoscenza ed osservanza, i componenti del Consiglio di Amministrazione, i componenti del Collegio Sindacale, i Dirigenti, i dipendenti e tutti i collaboratori con cui si intrattengono rapporti

contrattuali, a qualsiasi titolo, anche occasionali e/o soltanto temporanei, nonché tutti coloro che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con B.E.E. TEAM Spa.

2.3 Reati presupposto per i quali si stima vi sia un rischio di reato: elencazione delle fattispecie.

Reati previsti dall'articolo 24:

Art. 316 *bis* c.p. - Malversazione a danno dello Stato;

Art. 316 *ter* c.p. - Indebita percezione di erogazioni a danno dello Stato;

Art. 640, comma II, n. 1 c.p. - Truffa ai danni dello Stato;

Art. 640 *bis* c.p. - Truffa aggravata per il conseguimento di erogazioni pubbliche;

Art. 640 *ter* c.p. - Frode informatica.

Reati previsti dall'articolo 24 bis (introdotto dalla l. 48/08)

Art. 491 *bis* c.p. - Documenti informatici;

Art. 615 *ter* c.p. - Accesso abusivo ad un sistema informatico o telematico;

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;

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 *ter* c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;

Art. 635 *quater* c.p. - Danneggiamento di sistemi informatici o telematici;

Art. 635 *quinquies* c.p. - Danneggiamento di sistemi informatici o telematici di pubblica utilità;

Art 640 *quinquies* c.p. - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

Reati previsti dall'articolo 25:

Art. 317 c.p. – Concussione;

Art. 318 c.p. - Corruzione per un atto d'ufficio;

Art. 319 c.p. - Corruzione per un atto contrario ai doveri di ufficio;

Art. 319 *bis* c.p. - Circostanze aggravanti;

Art. 319 *ter* c.p. - Corruzione in atti giudiziari;

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, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri.

Reati previsti dall'articolo 25 ter (introdotto dal D. Lgs. 61/02)

Art. 2621 c.c. - False comunicazioni sociali;

Art. 2622 c.c. - False comunicazioni sociali in danno della società, dei soci o dei creditori;

Art. 2624 c.c. - Falsità nelle relazioni e nelle comunicazioni delle società di revisione;

Art. 2625 c.c. - Impedito controllo; (modificato dall'art. 37 del D.Lgs. 27 gennaio 2010, n. 39);

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. 2636 c.c. - Illecita influenza sull'assemblea;

Art. 2637 c.c. – Aggiotaggio.

Reati previsti dall'art. 25 sexies (introdotto dalla l. 62/05)

Art. 183 D. Lgs. 58/98 - Cause di non punibilità;

Art. 184 D. Lgs. 58/98 - Reato di abuso di informazioni privilegiate;

Art. 185 D. Lgs. 58/98 - Reato di manipolazione del mercato;

Art. 187 *bis* D. Lgs. 58/98 - Abuso di informazioni privilegiate;

Art. 187 *ter* D. Lgs. 58/98 - Manipolazione del mercato.

Reati previsti dall'art. 25 septies (introdotto dal D. Lgs. 123/07 e modificato dal D. Lgs. 81/08)

Art. 589 c.p. - Omicidio colposo;

Art. 590 c.p. - Lesioni personali colpose.

Reati previsti dall'art. 25 octies (introdotto dal D. Lgs. 231/07)

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.

2.4 Reati presupposto per i quali, in relazione all'attività svolta dalla Società e al suo contesto operativo, non si stima ipotizzabile un rischio di commissione ma su cui verrà comunque effettuata un'attività di vigilanza: elencazione delle fattispecie.

Reati previsti dall'art 25 bis (introdotto dalla l. 409/01)

Art. 453 c.p. - Falsità in monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate;

Art. 454 c.p. - Alterazione di monete;

Art. 455 c.p - Spendita e introduzione nello Stato, senza concerto, di monete falsificate;

Art. 457 c.p. - Spendita di monete falsificate ricevute in buona fede;

Art. 459 c.p. - Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati;

Art. 460 c.p. - Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo;

Art. 461 c.p. - Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata;

Art. 464 c.p. - Uso di valori di bollo contraffatti o alterati.

Reati previsti dall'art. 25 quater (introdotto dalla L. 7/03)

Art. 270 - ter c.p. - Associazioni con finalità di terrorismo internazionale;

Art. 270 - quinquies c.p. - Addestramento ad attività con finalità di terrorismo anche internazionale;

Art. 270 - sexies c.p. - Condotte con finalità di terrorismo;

Art. 414 c.p. - Istigazione a delinquere.

Reati previsti dall' art. 25 quater -1 (introdotto dalla l. 7/06):

Art. 583 bis c.p. - Pratiche di mutilazione degli organi genitali femminili.

Reati previsti dall'art. 25 quinquies (introdotto dalla l. 228/03)

Art. 600 c.p. - Riduzione o mantenimento in schiavitù o in servitù;

Art. 600 bis c.p. - Prostituzione minorile;

Art. 600 ter c.p. - Pornografia minorile;

Art. 600 quater c.p. - Detenzione di materiale pornografico;

Art. 600 quater bis c.p. – Pornografia virtuale

Art. 600 quinquies c.p. - Iniziative turistiche volte allo sfruttamento della prostituzione minorile;

Art. 601 c.p. - Tratta di persone;

Art. 602 c.p. - Acquisto o alienazione di schiavi.

Reati previsti dalla l. 146/2006 - Reati transnazionali:

Art. 377-bis c.p. - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;

Art. 378 c.p. - Favoreggiamento personale;

Art. 416 c.p. - Associazione per delinquere;

Art.416 *bis* c.p. - Associazione di tipo mafioso;

Art. 291 *quater* DPR 23 gennaio 1973 n.43 - Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri;

Art. 74 TU DPR 9 ottobre 1990 n.390 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

Art.12, comma 3, 3 *bis*, 3 *ter* e 5 TU D. Lgs.. 25 luglio 1998 n.286 - Traffico di migranti.

Reati previsti dal D.Lgs 58/98 (TUF) e successive modifiche

Art. 173 bis - Falso in prospetto

Reati previsti dall'art. 24 ter (introdotto dalla l. 94/2009 art. 2 co.29)

Art. 74 d.p.r. 309/90 - Associazione a delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope;

Art. 416 c.p. - Associazione a delinquere;

Art. 416 bis c.p. - Associazioni di tipo mafioso e delitti commessi per agevolare tali associazioni (art. 7 legge 203/91);

Art. 629 c.p. - sequestro di persona a scopo di rapina o di estorsione.

Reati previsti dall'art. 25-bis 1 (introdotto dalla l. 99/2009)

Art. 513 c.p.- Turbata libertà dell'industria o del commercio;

Art. 513-bis c.p. - Illecita concorrenza con minaccia o violenza";

Art. 514 c.p. - Frodi contro le industrie nazionali;

Art. 515 c.p. - Frode nell'esercizio del commercio;

Art. 516 c.p. - Vendita di sostanze alimentari non genuine come genuine;

Art. 517 c.p. - Vendita di prodotti industriali con segni mendaci;

Art. 517-ter c.p. - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale;

Art. 517-quater c.p. - Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari.

Reati previsti dall'articolo 25 ter (introdotto dal D. Lgs. 61/02)

Art. 2629 *bis* c.c. - Omessa comunicazione del conflitto di interessi.

Art. 2633 c.c. - Indebita ripartizione dei beni sociali da parte dei liquidatori;

Art. 2638 c.c. - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

Reati previsti dall'art. 25 novies (introdotto dalla l. 99/2009)

Art. 171, l. 633/1941 comma 1 lett a) bis - Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa;

Art. 171, l. 633/1941 comma 3) - reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE;

Art. 171-bis l. 633/1941 comma 1) predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori;

Art. 171-bis l. 633/1941 comma 2 - riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una

banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati;

Art. 171-ter l. 633/1941 - abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

Art. 171-septies l. 633/1941 - mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione;

Art. 171-octies l. 633/1941 - fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

Reati previsti dall'art. 25 novies (introdotto dalla l. 116/2009 art. 4)

Art. 377-bis c.p. - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

Reati previsti dall'art. 25 undecies (introdotto con il D.Lgs. 152/2006)

Art.192 – Abbandono e deposito incontrollato nel suolo e sul suolo di rifiuti.

Reati previsti dall'art. 25 duodecies (introdotto con il D.Lgs. 109/20)

In attuazione della Direttiva 2009/52/CE. Assunzione di lavoratori extracomunitari provvisti di permesso di soggiorno.

2.5 Approvazione e recepimento dei principi di riferimento del Modello

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma I, lett. a) del Decreto, in data 25 marzo 2011 il Consiglio di Amministrazione di B.E.E. TEAM Spa, su proposta dell'Organismo di Vigilanza, ha approvato gli **aggiornamenti** apportati al Modello.

3. ORGANISMO DI VIGILANZA

3.1 Identificazione dell'Organismo di Vigilanza

Il Decreto (art.6 lett. b) richiede, quale ulteriore condizione per ottenere l'esimente della responsabilità amministrativa, che il compito di vigilare sul funzionamento e sull'osservanza del Modello, nonché di curarne l'aggiornamento, sia affidato ad un organismo della Società dotato di autonomi poteri di iniziativa e di controllo.

1) Composizione dell'Organismo di Vigilanza

Il Consiglio di Amministrazione di B.E.E. TEAM spa., nella seduta del 28 aprile 2011, ha conferito la qualifica di Organismo di Vigilanza ai sensi dell'art. 6, lettera b del Decreto, ad un organismo collegiale composto dal Presidente, nella persona dell'avv. Sandro Ridolfi, dal dott. Marco Battistella e dal dott. Eugenio Fabris (Componenti).

2) I Componenti dell'Organismo di Vigilanza, chiamato a svolgere le funzioni che l'art. 6 lett. b possiedono – stando al dettato normativo e alle indicazioni ricavabili dai primi responsi giurisprudenziali – requisiti di:

- autonomia e indipendenza;
- professionalità;
- continuità d'azione;
- onorabilità

necessari per l'esercizio di tale funzione.

Le scelte dell'Organismo di Vigilanza sono insindacabili da parte delle istituzioni dell'ente stesso, pena il venir meno del requisito essenziale dell'autonomia propria dell'Organismo medesimo.

Tenuto conto delle peculiarità delle proprie attribuzioni e dei contenuti professionali specifici da esse richieste nello svolgimento dei compiti di vigilanza e controllo, l'Organismo di Vigilanza si può in ogni caso avvalere, sotto la sua diretta sorveglianza e responsabilità, di altre funzioni interne o di collaboratori esterni che, di volta in volta, si rendessero necessari in considerazione della specificità dei compiti affidati.

3.2. Regolamento sulle modalità di nomina, cessazione e sostituzione dei membri dell'Organismo di Vigilanza

Anche tenendo conto delle più recenti indicazioni inserite nelle "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001" emanate da Confindustria, B.E.E. TEAM Spa ha conferito all'Organismo di Vigilanza le seguenti attribuzioni, regolandone il funzionamento nel modo di seguito descritto, fermo restando il potere-dovere dell'Organismo di Vigilanza stesso di regolare in via autonoma il proprio funzionamento e la propria attività anche eventualmente modificando quanto qui previsto. Il "Regolamento" è depositato agli atti dell'OdV; in particolare si segnala:

1) Durata in carica

L'Organismo di Vigilanza dura in carica sino alla permanenza del Consiglio di Amministrazione che lo ha proposto all'Assemblea.

2) Modalità di nomina e revoca dell'Organismo di Vigilanza

L'Assemblea nella seduta del 28 aprile 2011 delega al Consiglio di Amministrazione:

- la facoltà di revocare il mandato ad uno (o a tutti) i membri dell'OdV nel caso in cui siano venuti meno i requisiti richiesti per l'esercizio di tale funzione, o quando si siano generate cause di incompatibilità per i membri dell'Organismo stesso o ancora quando l'operatività svolta ne abbia evidenziato la reale necessità;
- al termine di ciascun incarico dell'Organismo di Vigilanza, di provvedere al rinnovo verificando, prima di ogni nuova nomina, la sussistenza dei requisiti espressamente richiesti dal Decreto per ciascun membro dell'Organismo.

Il Consiglio di Amministrazione comunque valuta periodicamente l'adeguatezza dell'Organismo di Vigilanza in termini organizzativi e dei poteri conferiti. Il Consiglio di Amministrazione può peraltro, in qualunque momento, revocare, dandone successiva informativa all'Assemblea degli Azionisti, il mandato ad uno (o a tutti) i membri dell'Organismo di Vigilanza nel caso in cui siano venuti meno i requisiti di autonomia e indipendenza, professionalità, continuità d'azione ovvero di onorabilità necessari per l'esercizio di tale funzione o quando si siano generate cause di incompatibilità per i membri dell'Organismo stesso o ancora quando la valutazione periodica ne abbia evidenziato la reale necessità.

3.3 Funzioni e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono affidati i compiti di vigilare:

- sull'adeguatezza del Modello, ossia l'idoneità dello stesso a evitare i rischi di realizzazione dei reati;
- sull'aggiornamento del Modello, a seguito dei mutamenti nella realtà organizzativa e del quadro legislativo di riferimento;
- sull'effettività del Modello, che consiste nel verificare la coerenza tra comportamenti concreti e Modello istituito.

Pertanto, l'Organismo di Vigilanza deve provvedere a:

- verificare periodicamente la mappa delle aree a rischio reato al fine di adeguarla ai mutamenti delle attività e/o della struttura aziendale, nonché alle eventuali modifiche legislative. **A tal fine all'Organismo di Vigilanza devono essere segnalate da parte del management e da parte degli addetti alle attività di controllo, nell'ambito delle singole funzioni, le eventuali situazioni che possono esporre l'Azienda al rischio di reato;**
- effettuare periodicamente verifiche, sulla base di un programma annuale approvato dal Consiglio di Amministrazione, volte all'accertamento di quanto previsto dal Modello. In particolare verificare che:
  - le procedure di controllo siano poste in essere e documentate in maniera corretta;
  - i principi etici siano rispettati;
- verificare l'adeguatezza e l'efficacia del Modello nella prevenzione dei reati di cui al Decreto;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni):
  - per uno scambio di informazioni per tenere aggiornate le aree a rischio reato;
  - per tenere sotto controllo la loro evoluzione al fine di realizzare il costante monitoraggio;

B.E.E. Team spa *–Tutti i diritti riservati.*

- per i diversi aspetti attinenti l'attuazione del Modello (definizione di clausole contrattuali standard, formazione del personale, cambiamenti normativi ed organizzativi, ecc.);
- per garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace vengano intraprese tempestivamente;

- raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute sul rispetto del Modello, nonché aggiornare la lista delle informazioni che allo stesso devono essere trasmesse;
- mettere a disposizione e aggiornare, sulla rete interna aziendale, le informazioni relative al D. Lgs. 231/01 e al Modello.

La struttura così identificata deve essere in grado di agire nel rispetto dell'esigenza di recepimento, verifica ed attuazione del Modello.

All'Organismo di Vigilanza vengono attribuiti tutti i poteri e le capacità di indagine necessari per intrattenere relazioni dirette e continuative con tutte le funzioni aziendali, che non potranno rifiutare la consegna della documentazione richiesta dall'Organismo di Vigilanza, fatti salvi i vincoli di legge in materia di privacy.

A tal fine, l'Organismo di Vigilanza deve avere libero accesso alle persone e a tutta la documentazione aziendale e la possibilità di acquisire dati ed informazioni rilevanti dai soggetti responsabili, senza restrizioni e senza la necessità di alcun consenso preventivo. Infine, all'Organismo di Vigilanza devono essere segnalate tutte le informazioni come meglio specificato al Capitolo 4 del presente Modello.

L'Organismo di Vigilanza deve essere inoltre dotato di adeguate risorse finanziarie delle quali dovrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti.

3.4 Reporting dell'Organismo di Vigilanza nei confronti degli organi societari

Sono previste le seguenti linee di riporto da parte dell'Organismo di Vigilanza:

- su base continuativa, nei confronti del Presidente del Consiglio di Amministrazione;
- su base periodica, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale;
- di carattere eventuale nel caso che, al di fuori delle attività di controllo periodico, l'Odv venga comunque a conoscenza di comportamenti in violazione delle procedure previste dal modello organizzativo, ovvero di altri comportamenti che integrino o possano integrare ipotesi di reati-presupposto: in tali casi, se il fatto è posto in essere da un soggetto apicale, l'informativa dovrà essere riferita al collegio sindacale; se il fatto è posta in essere da un soggetto non apicale, l'informativa sarà riferita al consiglio di amministrazione.

In ogni caso l'Organismo di Vigilanza ha la responsabilità di:

- comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
- redigere una relazione annuale che riferisca in ordine:
  - alle attività svolte;

- allo stato di attuazione del Modello, segnalando - ove ritenuto opportuno o necessario - suggerimenti a proposito di modifiche da apportare al Modello stesso per mantenerlo adeguato alle esigenze normativamente poste;
- alle eventuali violazioni del Modello, anche se oggetto delle segnalazioni di carattere eventuale di cui si è in precedenza detto.

Nel caso in cui, dagli accertamenti svolti dall'Organismo, emergessero elementi che fanno risalire il reato o il tentativo di commissione del reato ad uno o più amministratori, sarà inevitabile che riferisca tempestivamente al Collegio Sindacale.

Il presidente del Consiglio di Amministrazione, l'Amministratore Delegato, il Consiglio di Amministrazione, il Collegio Sindacale hanno la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza il quale, a sua volta, ha la facoltà di richiedere, attraverso i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

Gli incontri con gli organi cui l'Organismo di Vigilanza riferisce devono essere verbalizzati e copia dei verbali deve essere custodita dall'OdV stesso ed inviata agli organi di volta in volta coinvolti.

4. OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Al fine di agevolare l'attività di vigilanza sull'effettività e sull'efficacia del Modello, l'Organismo di Vigilanza è destinatario di tutte le segnalazioni e le informazioni ritenute utili a tale scopo.

Gli amministratori, i dirigenti, i dipendenti, consulenti e partner di B.E.E. TEAM Spa sono tenuti ad informare tempestivamente l'Organismo di Vigilanza in ordine ad ogni violazione o sospetto di violazione del Modello, dei suoi principi generali e del Codice Etico previsto dal D. Lgs. 231/2001, nonché in ordine alla loro inidoneità, inefficacia e ad ogni altro aspetto potenzialmente rilevante.

In particolare, tutti i soggetti di cui sopra sono tenuti a trasmettere tempestivamente all'Organismo di Vigilanza le informazioni concernenti:

- risultanze delle attività di controllo poste in essere dalle funzioni aziendali dalle quali emergano criticità;
- anomalie o atipicità riscontrate dalle stesse funzioni;
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. 231/2001;
- avvio di contenzioso giudiziale e/o stragiudiziale da parte di Clienti/Fornitori;
- comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato di cui al D. Lgs. 231/2001 (ad es.: provvedimenti disciplinari avviati/attuati nei confronti di dipendenti);
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa, ovvero per altri reati in

qualche misura collegabili con i c.d. reati-presupposto (ad es. reati in materia tributaria che possono essere collegati a reati come le false comunicazioni sociali);

- relazioni/comunicazioni interne ovvero di commissioni d'inchiesta comunque denominate, dalle quali emergano responsabilità per le ipotesi di reato di cui al D. Lgs. 231/2001;
- notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza - nell'ambito dei procedimenti disciplinari svolti - delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- prospetti riepilogativi degli appalti affidati a seguito di gare, o trattativa privata;
- le notizie relative a cambiamenti organizzativi (organigrammi);
- gli aggiornamenti del sistema delle deleghe e dei poteri;
- i mutamenti nelle situazioni di rischio o potenzialmente a rischio (es.: costituzione di "fondi a disposizione di organi aziendali", ecc.);
- le eventuali comunicazioni della società di revisione riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni;
- copia dei verbali delle riunioni del Consiglio di Amministrazione;
- qualsiasi incarico conferito, o che si intende conferire, alla società di revisione o a società ad esse collegate, diverso da quello concernente la revisione del bilancio;
- valutazioni in ordine alla scelta della società di revisione (in base ad elementi quali professionalità, esperienza nel settore, ecc. e non solo in base a criteri di economicità).
- qualunque ulteriore informazione o notizia, qualunque ne sia la fonte, attinente alla commissione dei reati previsti dal Decreto o comportamenti non in linea con il Modello predisposto.

Le segnalazioni devono essere effettuate in forma scritta non anonima su casella di posta elettronica appositamente dedicata e ad **accesso protetto e riservato al solo Organismo di Vigilanza (odv.beeteam@beeteam.it).**

E' garantita la riservatezza di tali comunicazioni e il loro anonimato e nessuna conseguenza negativa di alcun genere può riverberarsi sul soggetto autore della comunicazione a cagione della comunicazione stessa, eccettuato il caso di segnalazione consapevolmente e deliberatamente falsa e/o calunniosa.

L'Organismo di Vigilanza valuta le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine può ascoltare l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere.

4.1 Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'Organismo di Vigilanza in un apposito archivio riservato (informatico o cartaceo) per un periodo di 10 anni.

FORMAZIONE E COMUNICAZIONE

Ai fini dell'attuazione del presente Modello, la formazione del personale e la diffusione del documento sono gestite dalla Funzione Personale, in stretto coordinamento con l'Organismo di Vigilanza, e sono articolate sui livelli di seguito indicati:

- Personale Direttivo e con funzioni di rappresentanza dell'ente: corso di formazione iniziale circa i contenuti generali del Modello, l'istituzione dell'Organismo di Vigilanza, le istruzioni per l'utilizzo dei canali predisposti per le segnalazioni a questo destinate. Accesso al sito intranet dedicato all'argomento.
- Altro personale: nota informativa interna. Accesso al sito intranet dedicato all'argomento e successivi eventuali corsi/e-mail di aggiornamento.
- Neo Assunti: consegna del Codice Etico all'atto dell'assunzione e valutazione della loro collocazione in aree a rischio, per cui potrebbe rendersi necessaria una formazione specifica. Inserimento nel percorso formativo sopra previsto per l'"altro personale" o il "personale direttivo" a seconda dei casi che ricorrono.

Informativa a collaboratori Esterni e Partners

B.E.E. TEAM Spa promuove la conoscenza e l'osservanza del Modello anche tra i propri partner commerciali e finanziari, consulenti, collaboratori a vario titolo, clienti e fornitori.
A costoro verranno pertanto fornite, oltre ad una copia del Codice Etico, apposite informative sui principi, le politiche e le procedure che B.E.E. TEAM Spa ha adottato sulla base del presente Modello, nonché i testi delle clausole contrattuali che, coerentemente a detti principi, politiche e procedure, verranno adottate dalla Società.

6. SISTEMA DISCIPLINARE

6.1 La funzione del sistema disciplinare

L'art. 6 D. Lgs. 231/2001 – facendo dipendere l'esclusione della responsabilità diretta dell'ente dall'adozione e dalla efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire la realizzazione degli illeciti penali indicati nello stesso decreto legislativo – ha previsto l'introduzione di "un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello", che diviene quindi necessaria parte integrante del modello organizzativo complessivamente considerato.

B.E.E. Team spa *–Tutti i diritti riservati.*

Emerge, quindi, la rilevanza del sistema disciplinare quale fattore essenziale del Modello Organizzativo ai fini dell'applicabilità all'ente dell"esimente" prevista dalla citata disposizione di legge.

6.2 Il sistema disciplinare

6.2.1 Il sistema disciplinare: dipendenti e collaboratori

Il sistema disciplinare identifica le infrazioni ai principi, ai comportamenti e agli elementi specifici di controllo contenuti nel Modello Organizzativo, e a queste sono associate le sanzioni previste per il personale dipendente.

Il complesso di infrazioni e sanzioni correlate è specificamente definito nella sottostante tabella.

Il Modello Organizzativo, comprensivo del sistema disciplinare, in ragione della sua valenza applicativa, **dovrà essere formalmente dichiarato vincolante per tutti i dipendenti e, pertanto, essere esposto, così come previsto dall'art. 7, co. 1, l. 300/1970, "mediante affissione in luogo accessibile a tutti".**

Resta fermo che le sanzioni disciplinari per il personale dipendente terranno conto in sede applicativa del principio di proporzionalità previsto dall'art. 2106 c.c., considerandosi, per ciascuna fattispecie, la gravità oggettiva del fatto costituente infrazione disciplinare, il grado di colpa, l'eventuale reiterazione di un medesimo comportamento, nonché l'intenzionalità del comportamento stesso.

Resta salva la facoltà per la società di rivalersi per ogni danno e/o responsabilità che alla stessa possano derivare da comportamenti di dipendenti e collaboratori esterni in violazione del Modello Organizzativo.

B.E.E. Team spa *–Tutti i diritti riservati.*

SISTEMA DISCIPLINARE

INFRAZIONI	LAVORATORI DIPENDENTI NON DIRIGENTI	DIRIGENTI
Inosservanza sostanziale delle prescrizioni individuate nei "Principi Generali del Sistema di Controllo Interno (SCI)". (Cfr. Appendice punto B)	Richiamo verbale Ammonizione scritta Multa non superiore a tre ore della retribuzione base Sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni Licenziamento con preavviso	Idonee misure coerenti con il CCNL
Inosservanza dei comportamenti prescritti nei "Principi di comportamento con la Pubblica Amministrazione" (Cfr. Appendice punto C)	Multa non superiore a tre ore della retribuzione base Sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni Licenziamento con preavviso	Idonee misure coerenti con il CCNL
Inosservanza degli elementi specifici di controllo previsti negli SCI per negligenza e senza l'esposizione della Società ad una situazione oggettiva di pericolo.	Ammonizione scritta Multa non superiore a tre ore della retribuzione base Sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni Licenziamento con preavviso	Idonee misure coerenti con il CCNL
Omissione di comunicazione dovuta all'OdV come indicata negli SCI.	Richiamo verbale Ammonizione scritta Multa non superiore a tre ore della retribuzione base Sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni Licenziamento con preavviso Licenziamento senza preavviso	Idonee misure coerenti con il CCNL
Comportamenti a rischio (così come elencati negli SCI dei processi operativi e strumentali) tenuti nei confronti dei funzionari PA.	Richiamo verbale Ammonizione scritta Multa non superiore a tre ore della retribuzione base Sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni	Idonee misure coerenti con il CCNL
Comportamento a rischio (così come elencati negli SCI dei processi operativi e strumentali) che si è in concreto tradotto in un atto che espone la Società anche a una situazione oggettiva di pericolo.	Sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni Licenziamento con preavviso Licenziamento senza preavviso	Idonee misure coerenti con il CCNL
Comportamento diretto in modo univoco ed intenzionale al compimento di un reato sanzionato nel Decreto.	Licenziamento con preavviso Licenziamento senza preavviso	Idonee misure coerenti con il CCNL
Ogni altro e diverso comportamento tale da determinare potenzialmente l'imputazione a carico della Società delle misure previste dal Decreto.	Multa non superiore a tre ore della retribuzione base. Sospensione da l lavoro e dalla retribuzione fino ad un massimo di tre giorni Licenziamento con preavviso Licenziamento senza preavviso	Idonee misure coerenti con il CCNL
Comportamento che ha determinato l'applicazione delle misure previste dal Decreto.	Sospensione dal lavoro e dalla retribuzione fino ad un massimo di dieci giorni Licenziamento con preavviso Licenziamento senza preavviso	Idonee misure coerenti con il CCNL

B.E.E. Team spa *–Tutti i diritti riservati.*

6.2.2 Il sistema disciplinare: soggetti apicali

Informativa dell'Organismo di Vigilanza al Consiglio di Amministrazione e Collegio Sindacale per l'opportuna valutazione.
Per Amministratori e Sindaci il Consiglio di Amministrazione potrà proporre alla successiva Assemblea la revoca per giusta causa del Consigliere o Sindaco.

6.2.3 Le misure nei confronti dei lavoratori autonomi/collaboratori

L'inosservanza delle norme indicate nel Modello di organizzazione, gestione e controllo adottato da B.E.E. TEAM Spa ai sensi del D. Lgs. 231/2001, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte di ciascun lavoratore autonomo/collaboratore, può determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, ferma restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

6.2.4 Le misure nei confronti dei soggetti aventi rapporti contrattuali/commerciali con B.E.E. TEAM Spa.

L'inosservanza delle norme indicate nel Modello di organizzazione, gestione e controllo adottato da B.E.E. TEAM Spa ai sensi del D. Lgs. 231/2001, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte dei soggetti aventi rapporti contrattuali/commerciali con B.E.E. TEAM Spa, può determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, fermo restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

6.2.5 Le misure nei confronti dei membri dell'Organismo di Vigilanza

Qualora il Consiglio di Amministrazione fosse informato in merito a violazioni del presente Modello da parte di uno o più membri dell'Organismo di Vigilanza, provvederà ad assumere le iniziative ritenute più idonee.

6.3 Soggetti titolati a comminare i provvedimenti disciplinari

Il sistema disciplinare è soggetto a costante verifica e valutazione da parte dell'Organismo di Vigilanza.

Per l'applicazione delle sanzioni disciplinari previste, l'Organismo di Vigilanza riferisce all'organo competente all'irrogazione della sanzione (Consiglio di Amministrazione e Collegio Sindacale quando si tratti di soggetti apicali, Responsabile della Funzione Personale quando si tratti di dipendenti in posizioni non apicali; Responsabile della funzione interessata quando si tratti di soggetti terzi rispetto alla Società). Tramite la Funzione del Personale, responsabile della concreta applicazione delle misure disciplinari previste, verranno irrogate le relative sanzioni.

7. MODELLO E CODICE ETICO

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

Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma dalla Società ed è suscettibile di applicazione sul piano generale da parte della Società allo scopo di esprimere i principi di "deontologia aziendale" che B.E.E. TEAM Spa riconosce come propri e all'osservanza dei quali richiama tutti gli Esponenti Aziendali;
- il Modello, declinando in concreto i principi contenuti nel Codice Etico, risponde alle specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati o di illeciti amministrativi, nonché condotte o comportamenti ad essi prodromici.

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "A"

Aree di attività nel cui ambito possono essere commessi i reati ex artt. 24 e 25 del D. Lgs. 231/2001

B.E.E. Team spa *–Tutti i diritti riservati.*

1. FUNZIONE DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Destinatari del Modello Organizzativo, come già definiti nella Parte Generale, coinvolti nei Processi Sensibili e più precisamente specificati nell'analisi della aree potenziali di rischio di cui al successivo par. 4.

Obiettivo della presente Parte Speciale è che i suddetti soggetti adottino regole di condotta conformi a quanto prescritto dalla stessa, allo scopo di impedire la commissione dei reati in essa considerati.

2. TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

I reati in danno della P.A. di cui agli artt. 24 e 25 del D. Lgs. 231/01, sono:

- indebita percezione di contributi, finanziamenti o altre erogazioni da parte di un ente pubblico (art. 316-ter c.p.);
- truffa in danno dello Stato o d'altro ente pubblico (art. 640, 1° comma, n. 1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
- corruzione per un atto d'ufficio (art. 318 c.p.);
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- corruzione in atti giudiziari (art. 319-ter c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- corruzione di persone incaricate di pubblico servizio (art. 320 c.p.);
- concussione (art. 317 c.p.);
- malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.);
- peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.).

3. RESPONSABILI INTERNI E SCHEDE DI EVIDENZA

I destinatari della presente Parte Speciale che intrattengono rapporti con la Pubblica Amministrazione divengono responsabili interni di ogni singola operazione a rischio da loro direttamente svolta o attuata nell'ambito della funzione a loro facente capo. Detti Responsabili:

- divengono i soggetti referenti dell'operazione a rischio;
- sono responsabili in particolare dei rapporti con la P.A., per le attività con essa svolta.

In tale veste, devono garantire un adeguato tracciamento documentale

- **delle decisioni assunte,**
- **delle trattative condotte,**
- **delle modifiche eventualmente apportate ad atti, accordi, contratti**

compilando e conservando ordinatamente a disposizione dell'Organismo di Vigilanza la specifica scheda di evidenza riportata in Allegato 1.

Devono inoltre segnalare tempestivamente, secondo le modalità previste dal presente Modello Organizzativo e dal quadro normativo aziendale, ogni eventuale situazione di rischio ai sensi del D. Lgs. 231/01, rilevata nello svolgimento delle proprie attività, oltre ad inviare, con la periodicità predefinita, i flussi informativi indicati nelle analisi delle potenziali aree di rischio esposte nel successivo par. 4, trattate in riferimento ai processi aziendali.

4. POTENZIALI AREE A RISCHIO E REGOLE DI COMPORTAMENTO

Le aree di attività nel cui ambito possono essere commessi i reati di cui al D. Lgs. 231/2001 riguardano i rapporti con la Pubblica Amministrazione e le situazioni in cui questa è comunque coinvolta (reati contro la Pubblica Amministrazione e contro il Patrimonio ex art. 24 e 25 del Decreto).

In considerazione della peculiarità delle attività svolte da B.E.E. TEAM Spa e della struttura interna adottata, per attivare un sistema di gestione dei rischi coerente con i requisiti imposti dal D. Lgs. 231/2001, sono state preliminarmente individuate le seguenti due categorie di aree oggetto di analisi:

- **AREE A RISCHIO REATO – PROCESSI OPERATIVI**, ossia aree nell'ambito delle quali, sulla base delle informazioni raccolte e condivise con i responsabili dell'area, sono intrattenuti rapporti con la Pubblica Amministrazione e dunque potenzialmente potrebbero essere commessi i reati ex artt. 24 e 25 del Decreto;
- **AREE DI SUPPORTO – PROCESSI STRUMENTALI**, ossia aree che gestiscono strumenti di tipo finanziario (e/o mezzi sostitutivi) che, pur non intrattenendo rapporti con la Pubblica Amministrazione, possono essere strumentali alla commissione dei reati nelle aree a rischio reato.

Le aree individuate, suddivise come sopra indicato, sono:

PROCESSI OPERATIVI

1)	**Gestione verifiche ed ispezioni. Gestione rapporti con PA. (pag. 36).**
2)	**Obblighi previdenziali (pag. 38).**
3)	**Bilancio e Bilancio consolidato (vedi parte speciale B).**
4)	**Sicurezza sui luoghi di lavoro ecc. (vedi parte speciale C).**
5)	**Smaltimento rifiuti (vedi parte speciale G)**

PROCESSI STRUMENTALI

6)	**Selezione del personale (pag. 40).**
7)	**Finanza dispositiva e tesoreria (pag. 42).**

B.E.E. Team spa *–Tutti i diritti riservati.*

8) **Consulenze (pag. 443).**
9) **Gestione contenzioso e precontenzioso (pag. 46)**
10) **Acquisto di beni e servizi (pag. 48).**

I processi sopra individuati, esposti al rischio di commissione dei reati v/ la P.A. analizzati nelle schede sottostanti, possono altresì dare luogo, sempre in relazione alle medesime fattispecie di reato, anche ai delitti di criminalità organizzata. Ne deriva che i protocolli di prevenzione e controllo, indicati nelle citate schede, costituiscono un presidio di contrasto anche in riferimento ai reati associativi, oltre agli specifici principi di carattere generale di cui alla Parte Speciale F.

Analogamente, i protocolli di controllo indicati nelle schede costituiscono - in aggiunta agli specifici principi di carattere generale di cui alla Parte Speciale D - un presidio di contrasto anche del rischio di commissione dei reati di riciclaggio e uso di capitali illeciti cui sono esposti alcuni dei processi sopra indicati, in particolare:

Finanza dispositiva e tesoreria.

Consulenze.

Acquisti di beni e servizi.

PROCESSI OPERATIVI

1. GESTIONE VERIFICHE ED ISPEZIONI. GESTIONE RAPPORTI CON PA.

DESCRIZIONE PROCESSO

I processi relativi alla gestione dei rapporti con Istituzioni ed Enti di Controllo nel corso di verifiche ed ispezioni si riferiscono a:

- Obblighi di notifica/informativa nei confronti di Autorità indipendenti/ Enti di vigilanza e controllo (ad. Es. Privacy, Consob).
- Adempimenti periodici richiesti da normative civilistiche, fiscali, previdenziali, sanitarie, di lavoro, ecc.
- Comunicazione di dati societari /aziendali di qualsiasi natura (Ufficio Catasto, Ufficio del Registro, ecc.);
- Richieste di autorizzazione e di concessione (es.: spazi per installazioni, concessioni edilizie, ecc.)

Tali processi presentano uno sviluppo sostanzialmente analogo articolato nelle seguenti fasi:

- Istruttoria interna e predisposizione documentale.
- Presentazione della richiesta/adempimento all'autorità pubblica.
- Gestione del rapporto con l'autorità pubblica interessata, compreso verifiche ed ispezioni ed eventuali accertamenti, sanzioni e/o contenziosi.

REATI ASSOCIABIILI

In relazione a questo processo, i reati ipotizzabili, in linea di principio, potrebbero essere: **corruzione e truffa a danno dello Stato,** v/ la P.A., e di **criminalità organizzata** (v. anche Parte Speciale F).

A titolo esemplificativo si possono configurare le seguenti modalità di commissione dei reati di cui si tratta:

- offerta o promessa ad un pubblico agente di un'utilità non dovuta o di una somma di denaro per favorire l'ottenimento di una licenza o di un'autorizzazione, in mancanza dei requisiti necessari (reato di corruzione);
- offerta o promessa di un'utilità indebita ad un militare della Guardia di Finanza in sede di accertamento fiscale, direttamente o tramite l'intermediazione di personale o intermediario autorizzato della società, al fine di ottenere un esito favorevole e più celere dell'accertamento, in cambio dell'impegno al pagamento di una somma di denaro (reato di corruzione);
- offerta o promessa di un'utilità indebita ad un funzionario di una autorità di vigilanza (anche straniera) al fine di ottenere un trattamento favorevole per la società in sede di contenzioso amministrativo (ad esempio, relativo all'applicazione di una sanzione amministrativa, in cambio della corresponsione di una somma di denaro, ovvero di altra utilità (ad esempio, l'impegno all'assunzione presso la società di un familiare) (reato di corruzione);

B.E.E. Team spa *–Tutti i diritti riservati.*

- offerta o promessa di un'utilità indebita ad un ausiliario di un magistrato al fine di indurlo ad occultare un documento sfavorevole per la società, contenuto nel fascicolo del procedimento, in cambio del pagamento di una somma di denaro (reato di corruzione);
- offerta o promessa di un'utilità indebita ad un funzionario di enti previdenziali, dell'ASL o dell'Ispettorato del lavoro, in sede di accertamenti o verifiche, in cambio della promessa di una somma di denaro o di altra utilità (reato di corruzione);
- induzione in errore dell'autorità giudiziaria, autorità amministrative con funzioni ispettive e di verifica, amministrazione finanziaria ecc., in vista dell'ottenimento di vantaggi per la società (reato di truffa aggravata ai danni dello Stato/frode informatica ai danni dello Stato);
- offerta o promessa ad un pubblico agente di un'utilità non dovuta al fine di ottenere un provvedimento autorizzativo in materia di sicurezza e igiene sul lavoro e/o gestione dei rifiuti, in cambio di una somma di denaro o di altra utilità (reato di corruzione).

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sull'elemento essenziale della tracciabilità degli atti. In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Effettuazione di verifica di congruenza fra quanto autorizzato, quanto realizzato e quanto dichiarato alla Pubblica Amministrazione ai fini del pagamento dei corrispettivi previsti.
- Tracciabilità degli atti e delle fonti informative nelle singole fasi dei processi con specifico riferimento ad impiego di risorse e tempi.
- Esistenza di direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con i dipendenti della Pubblica Amministrazione.
- Formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla società.
- Selezione ed utilizzo di fornitori da albo fornitori qualificati e modalità operative finalizzate a valutazione di qualità anche nei confronti dei professionisti esterni di cui ci si avvale.

Devono, inoltre, essere definite adeguate modalità di *escalation* autorizzativa per la gestione delle eventuali deroghe ai principi sopra esposti.

INDICAZIONI COMPORTAMENTALI

Non adottare comportamenti a rischio di reato e/o contrari al Codice Etico e ai Principi di Comportamento con la Pubblica Amministrazione, in tutte le fasi del processo.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Flusso 1: Elenco delle contestazioni e dei contenziosi promossi dalla Pubblica Amministrazione.

3. OBBLIGHI PREVIDENZIALI

DESCRIZIONE PROCESSO

Il processo si riferisce alle attività svolte per ottemperare agli adempimenti prescritti dalle leggi, in relazione ai trattamenti previdenziali del personale dipendente, dei collaboratori coordinati e continuativi e la relativa disciplina sanzionatoria.

Il processo si articola nelle seguenti fasi:

- **determinazione degli importi da versare (sulla base delle retribuzioni e dei compensi) e** predisposizione delle dichiarazioni prescritte dalla legge (DM10, F24, ecc.);
- approvazione delle dichiarazioni per gli Enti;
- invio (prevalentemente telematico) dei moduli e versamento dei relativi importi;
- visite ispettive (eventuali).

REATI ASSOCIABIILI

In relazione a questo processo, i **reati ipotizzabili**, in linea di principio, potrebbero essere: **corruzione, indebita percezione di erogazioni, malversazione e truffa a danno Stato.**

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sugli elementi essenziali della tracciabilità degli atti. In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica della correttezza dei dati forniti dai sistemi di amministrazione del personale.
    - Verifica di conformità fra dati forniti dai sistemi di amministrazione del personale e dati dichiarati.
    - Tracciabilità degli atti e delle fonti informative nelle singole fasi del processo.

INDICAZIONI COMPORTAMENTALI

Non adottare comportamenti contrari al Codice Etico e alle Linee di Condotta, in tutte le fasi del processo ed in particolare nelle seguenti attività:

- Determinazione degli importi e predisposizione delle dichiarazioni;
    - in sede di raccolta della documentazione e predisposizione della dichiarazione quando tali comportamenti siano diretti a rappresentare alla P.A. informazioni non vere e/o non complete o ad eludere obblighi di legge;
- Visite ispettive da parte della P.A.;
    - in sede delle suddette visite, quando tali comportamenti siano finalizzati ad influenzare indebitamente, nell'interesse della società, le relative risultanze (producendo un danno patrimoniale per la Pubblica Amministrazione).

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA/COMITATO DI CONTROLLO

Ogni struttura della funzione del personale deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco delle irregolarità riscontrate;

Flusso 2: elenco delle visite ispettive in corso;

Flusso 3: elenco delle visite ispettive concluse.

B.E.E. Team spa *–Tutti i diritti riservati.*

PROCESSI STRUMENTALI

1. SELEZIONE DEL PERSONALE

DESCRIZIONE PROCESSO

Il processo di selezione e gestione del personale è composto da tutte le attività necessarie alla costituzione del rapporto di lavoro tra la società ed una persona fisica. Il processo viene attivato per tutti i segmenti professionali di interesse (manager, professionalizzati, neo-laureati e neo-diplomati, personale con mansioni operative) e si articola, sostanzialmente, nelle seguenti fasi:

acquisizione e gestione dei curricula-vitae;

selezione;

formulazione dell'offerta ed assunzione.

REATI ASSOCIABILI

Il processo di selezione e assunzione costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di **corruzione,** v/ la P.A., e di **criminalità organizzata** (v. anche Parte Speciale F).

La selezione e l'assunzione di personale potrebbero costituire, infatti, un potenziale supporto alla commissione del reato verso pubblici ufficiali o incaricati di pubblico servizio per ottenerne favori nell'ambito dello svolgimento di altre attività aziendali (es.: ottenimento di licenze, rapporti con authority, ecc.).

Il reato si realizza con l'indebito ottenimento di vantaggi per la Società, attraverso la prospettata assunzione di un familiare del pubblico funzionario coinvolto (o, in futuro, dello stesso pubblico funzionario) ovvero del miglioramento indebito delle condizioni di un dipendente in quanto suo familiare (o comunque dallo stesso segnalato) (reati di corruzione).

Inoltre, nell'ambito della gestione del personale – effettuata direttamente o tramite contratto di outsourcing – assumono particolare rilievo i rapporti con i soggetti pubblici relativi agli adempimenti previdenziali ed assistenziali, nonché a quelli in materia di collocamento obbligatorio, medicina, gestione e trattamento dei dati personali.

A titolo esemplificativo, possono infine citarsi le seguenti ipotesi:

- promessa o dazione di utilità al fine di ottenere indebiti favoritismi in relazione all'assunzione di personale appartenente a categorie protette o agli adempimenti spettanti alla società in materia previdenziale e infortunistica (reato di corruzione);
- induzione in errore della pubblica amministrazione (anche attraverso l'abusivo accesso ad un sistema informatico e/o l'alterazione delle informazioni contenute in una banca dati) in merito all'assunzione di personale appartenente a categorie protette o agli adempimenti spettanti alla società in materia previdenziale e infortunistica (reati di truffa aggravata ai danni dello Stato/frode informatica ai danni dello Stato).

B.E.E. Team spa *–Tutti i diritti riservati.*

Il 9 agosto 2012 il Decreto Legislativo 16 luglio 2012, n. 109, che amplia i reati presupposto per la responsabilità amministrativa delle persone giuridiche, ha introdotto l'art. 25-*duodecies* all'interno del D.Lgs. 231/2001 ed ha esteso la responsabilità delle persone giuridiche anche al reato di **impiego di cittadini di paesi terzi con soggiorno irregolare.**

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** tra la Funzione del Personale e le funzioni utilizzatrici delle risorse, nonché dell'esistenza di **momenti valutativi tracciabili**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Nella fase "Acquisizione e gestione dei curricula -vitae", tracciabilità delle fonti di reperimento dei CV (ad es., società di head-hunting, e-recruitment, inserzioni, domande spontanee, presentazioni interne, ecc.).
- Nella fase di predisposizione della rosa delle candidature da sottoporre a selezione verificare il che il candidato sia in possesso di idoneo permesso di soggiorno. Successivamente monitoraggio delle scadenze.
- Nella fase "Selezione", rispetto del criterio della separazione organizzativa per le attività di valutazione delle candidature. In tale ambito:
  - prevedere distinte modalità di valutazione, "attitudinale" e "tecnica", del candidato;
  - assegnare la responsabilità di tali valutazioni a soggetti distinti (nelle realtà organizzative più strutturate, la valutazione a cura della funzione "tecnica" deve essere sempre accompagnata da quella della Funzione Risorse Umane);
  - richiedere la sottoscrizione formale delle suddette valutazioni da parte dei soggetti responsabili, a garanzia della tracciabilità delle scelte effettuate.
- Nella fase "Formulazione dell'offerta e assunzione":
  - procedere alla scelta in base a valutazione di idoneità;
  - in sede di sottoscrizione della lettera di assunzione, verificare l'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti.

Il processo deve prevedere, inoltre, modalità formali di escalation autorizzativa nei casi di deroga ai principi sopra elencati. Con riferimento alla formalizzazione della lettera di assunzione l'escalation prevede il ricorso al livello superiore (gerarchico o funzionale) rispetto a chi, di norma, è responsabile della firma.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

La Funzione del Personale deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco delle assunzioni effettuate in deroga ai principi sopra elencati e/o a seguito di segnalazioni interne.

Flusso 2: elenco delle assunzioni effettuate di personale di paesi terzi.

2. FINANZA DISPOSITIVA E TESORERIA

DESCRIZIONE PROCESSO

Il processo si riferisce alle attività riguardanti i flussi monetari e finanziari in uscita aventi l'obiettivo di assolvere le obbligazioni di varia natura delle unità operative della Società.

I flussi suddetti si articolano sostanzialmente in due macro-gruppi:

- Flussi di natura **ordinaria**, connessi ad attività/operazioni correnti (ad es., flussi monetari in uscita relativi a: acquisti di beni, servizi e licenze, oneri finanziari, fiscali e previdenziali, stipendi e salari).
- Flussi di natura **straordinaria**, connessi alle operazioni di tipo finanziario (ad es., sottoscrizioni e aumenti di capitale sociale, finanziamenti, cessioni di credito, operazioni in valuta estera e sui derivati - swap, futures, ecc.).

Il processo si articola nelle seguenti fasi:

- pianificazione del fabbisogno finanziario periodico e/o spot sulla base di eventuale comunicazione inoltrate dalle altre funzioni;
- predisposizione delle disponibilità finanziarie, da parte della Tesoreria, alle date prestabilite presso gli istituti bancari di riferimento;
- richiesta dell'ordine di pagamento o di messa a disposizione;
- destinazione dell'importo, conformemente alle disposizione della società.

REATI ASSOCIABILI

Il processo di gestione della tesoreria costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di **corruzione v/ la P.A, nonché di riciclaggio ed uso di capitali illeciti** (v. anche Parte Speciale D) **e di criminalità organizzata** (v. Parte Speciale F).

Questo processo potrebbe, infatti, costituire supporto alla costituzione di disponibilità finanziarie occulte - sia in Italia che all'estero - destinabili pubblici agenti in vista dell'ottenimento di vantaggi indebiti in favore della Società (corruzione) , ovvero a scopo di riciclaggio e/o uso di capitali illeciti, ad esempio attraverso:

- pagamenti di ordini di acquisto, consulenze, prestazioni con corrispettivi fittiziamente maggiorati o per acquisti/prestazioni, anche in parte, inesistenti;
- pagamenti in contanti in violazione degli obblighi di legge;
- pagamenti a soggetti non adeguatamente identificati o non coincidenti con le organizzazioni che hanno fornito i beni, i servizi e le prestazioni;
- incassi e pagamenti con strumenti finanziari particolarmente complessi e/o estranei allo scopo aziendale.

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e dei **livelli autorizzativi** da associarsi alle operazioni.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - richiesta dell'ordine di pagamento;
  - predisposizione del pagamento dopo le verifiche di rito;
  - effettuazione del pagamento;
  - controllo/riconciliazioni a consuntivo.
- Esistenza di livelli autorizzativi sia per la richiesta, che per l'ordine di pagamento o di messa a disposizione, articolati in funzione della natura dell'operazione (ordinaria/straordinaria) e dell'importo.
- Esistenza di un flusso informativo sistematico che garantisca il costante allineamento fra procure, deleghe operative e profili autorizzativi residenti nei sistemi informativi.
- Esistenza e diffusione di specimen di firma in relazione ai livelli autorizzativi definiti per la richiesta.
- Effettuazione di periodica attività di riconciliazione, sia di eventuali conti intercompany, sia dei conti intrattenuti con banche.
- Tracciabilità degli atti e delle singole fasi del processo.

Eventuali modalità non standard (relative sia a operazioni di natura ordinaria che straordinaria) devono essere considerate "in deroga" e soggette, pertanto, a criteri di autorizzazione e controllo specificamente definiti riconducibili a:

- Individuazione del soggetto che può richiedere l'operazione;
- Individuazione del soggetto che può autorizzare l'operazione;
- Indicazione, a cura del richiedente, della motivazione;
- Designazione (eventuale) della risorsa abilitata all'effettuazione/autorizzazione dell'operazione attraverso procura ad hoc.

FLUSSI INFORMATIVI VERSO ORGANISMO DI VIGILANZA/COMITATO DI CONTROLLO

Il Responsabile Amministrazione Finanza e Controllo deve comunicare, per quanto di competenza e con periodicità definita, :

Flusso 1: Flussi finanziari significativi rispetto al normale andamento del business.

Flusso 2: Elenco dei flussi monetari e/o finanziari non standard (operazioni straordinarie come sottoscrizioni e aumenti di capitale sociale, finanziamenti, cessioni di credito, operazioni in valuta estera e sui derivati - swap, futures, ecc.) realizzati nel periodo.

3. CONSULENZE

DESCRIZIONE PROCESSO

Il processo riguarda l'assegnazione di incarichi per consulenze e prestazioni professionali a soggetti terzi e pertanto si configura, pur nella specificità dell'oggetto contrattuale, come un processo d'acquisizione, articolato nelle seguenti fasi:

- definizione del budget;
- emissione della Richiesta di Consulenza/Prestazione Professionale;
- scelta del Consulente;
- contrattualizzazione;
- gestione operativa del contratto;
- rilascio benestare, contabilizzazione e pagamento fatture.

REATI ASSOCIABILI

Il processo di assegnazione di incarichi di consulenza/prestazione professionale costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il **reato di corruzione v/ la P.A, nonché di riciclaggio ed uso di capitali illeciti** (v. anche Parte Speciale D) **e di criminalità organizzata** (v. Parte Speciale F).

Il conferimento di consulenze può infatti risultare strumentale alla corresponsione di indebite utilità a favore di pubblici ufficiali o incaricati di pubblico servizio: si pensi, ad esempio, al caso dell'attribuzione di un fittizio contratto di consulenza – e del riconoscimento del relativo compenso – a favore di un pubblico agente (o di persone fisiche o giuridiche allo stesso riconducibili) al fine di compensarne gli indebiti favori o di ottenere un indebito vantaggio.

Inoltre, attraverso il conferimento di contratti di consulenza fittizi o a prezzi superiori a quelli di mercato, la Società può costituire indebite provviste finanziarie da utilizzare in vista del pagamento di pubblici agenti.

Particolare attenzione deve essere altresì rivolta al conferimento di contratti di consulenza o prestazione professionale a favore di soggetti terzi che potrebbero, al fine di avvalorare la propria attività agli occhi della Società, utilizzare una parte dei compensi pattuiti all'attribuzione di indebiti vantaggi a favore di pubblici agenti e a vantaggio della Società

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sui due elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** , a garanzia della trasparenza delle scelte effettuate e del servizio ricevuto.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - richiesta della consulenza/prestazione,

- autorizzazione,
- definizione contrattuale,
- certificazione dell'esecuzione dei servizi (rilascio benestare),
- effettuazione del pagamento.

- Esistenza di requisiti professionali, legali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e di meccanismi di valutazione complessiva del servizio reso.
- Espletamento di adeguata attività selettiva fra diversi offerenti e di comparazione delle offerte (sulla base di criteri oggettivi e documentabili).
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati.
- Per consulenze/prestazioni professionali svolte da soggetti terzi incaricati di rappresentare B.E.E. TEAM Spa nei confronti della P.A. deve essere prevista una specifica clausola che li vincoli all'osservanza dei principi etico-comportamentali adottati dalla Società.
- Esistenza di livelli di approvazione per la formulazione delle richieste di consulenza/prestazione e per la certificazione/validazione del servizio reso nonché di trasparenti livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni.
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire, la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.
- Le relazioni periodiche da rendere alla Società in merito al rispetto dei compiti e delle responsabilità assegnati.

Devono, inoltre, essere definite modalità operative e connessi meccanismi di escalation autorizzativa per eventuali deroghe ai principi sopra riportati, laddove ritenuto necessario, ad esempio per esigenze di riservatezza e tempestività.

FLUSSI INFORMATIVI VERSO ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni utilizzatrici (o delegate a gestire il processo di acquisizione delle consulenze) devono comunicare, con periodicità definita, quando indicato:

Flusso 1: Consuntivo attività di consulenza/prestazioni professionali suddivise per Consulente.

4. GESTIONE CONTENZIOSO E PRECONTENZIOSO.

DESCRIZIONE PROCESSO

Il processo concerne tutte le attività necessarie a prevenire o dirimere una controversia con soggetti terzi; tali attività sono finalizzate, in particolare, a consentire di accordarsi con terzi, mediante reciproche concessioni, evitando di instaurare un procedimento giudiziario.

Le controversie possono derivare sia da un rapporto contrattuale, sia da responsabilità extracontrattuali (ad es., insorgere della lite a seguito di danni provocati da terzi all'Azienda e viceversa).

Il processo si articola nelle seguenti fasi:

- analisi dell'evento da cui deriva la controversia;
- esame dell'esistenza dei presupposti per addivenire alla transazione;
- gestione delle attività finalizzate alla definizione e formalizzazione della transazione;
- redazione, stipula ed esecuzione dell'accordo transattivo.

REATI ASSOCIABILI

Il processo relativo agli accordi transattivi costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di **corruzione**, v/ la P.A., e di **criminalità organizzata** (v. anche Parte Speciale F).

La gestione anomala del processo transattivo potrebbe costituire, infatti, una potenziale modalità di predisposizione di mezzi finanziari utili per assicurare la "provvista" anche ai fini della commissione di reati rilevanti ai sensi del D. Lgs. 231/01.

Nell'ambito della gestione delle controversie può, ad esempio, configurarsi il reato di corruzione attraverso

- l'offerta o promessa di un'utilità indebita ad un magistrato o ad un componente del collegio arbitrale, anche tramite l'intermediazione del legale di fiducia della società, al fine di ottenere una pronuncia in sede civile di condanna delle controparte, in cambio della promessa di una somma di denaro;
- l'offerta o promessa di un'utilità indebita ad un magistrato per ottenere una pronunzia favorevole alla società, in cambio della promessa di vantaggi indebiti (ad esempio, la messa a disposizione di un appartamento, o l'attribuzione di consulenze fittizie retribuite dalla società);
- offerta o promessa di un'utilità indebita ad un Pubblico Ministero, al fine di ottenere la revoca di un provvedimento di sequestro avente ad oggetto beni della società, disposto nell'ambito di un procedimento penale, in cambio della promessa di una somma di denaro o di altra utilità.

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** fra le fasi chiave del processo e della **tracciabilità delle fasi** a garanzia delle scelte effettuate alla base dell'accordo transattivo.

B.E.E. Team spa *–Tutti i diritti riservati.*

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di **responsabilità differenziate** fra:
  - **gestione operativa** del processo aziendale legato all'accordo transattivo,
  - **gestione della trattativa** e formalizzazione dell'accordo transattivo.
- Esistenza, presso i soggetti coinvolti, di evidenza documentale delle singole fasi del processo (richiesta, gestione, formalizzazione ed esecuzione dell'accordo).
- Esistenza di livelli autorizzativi coerenti con il sistema di procure aziendali per la stipulazione ed esecuzione degli accordi transattivi.
- Esistenza di criteri quali/quantitativi per il ricorso ad accordi transattivi in alternativa alla gestione della controversia in sede giudiziale.

Devono essere, inoltre, previste modalità di escalation autorizzativa per la gestione delle deroghe (particolarmente per il supero delle soglie di cui al punto precedente), con necessario parere della funzione Legale.

FLUSSI INFORMATIVI VERSO ORGANISMO DI VIGILANZA

Il Vertice aziendale deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco delle transazioni significative (oltre un prestabilito valore soglia), e di quelle gestite in deroga.

5. ACQUISTO DI BENI E SERVIZI

DESCRIZIONE PROCESSO

Il processo di acquisizione di beni e servizi si articola nelle seguenti fasi:

- pianificazione fabbisogni in relazione al budget e definizione del Programma d'Acquisto;
- emissione della Richiesta di Acquisto;
- scelta della fonte d'acquisto e definizione del contratto;
- gestione operativa del contratto/ordine (esecuzione prestazioni/consegna beni);
- rilascio benestare;
- contabilizzazione e pagamento fatture.

REATI ASSOCIABILI

Il processo di acquisizione di beni e servizi costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di **corruzione v/ la P.A., nonché quelli di riciclaggio e uso di capitali illeciti** (v. anche Parte Speciale D) **e di criminalità organizzata** (v. Parte Speciale F)..

Il reato di corruzione potrebbe essere commesso attraverso la gestione non trasparente del processo di acquisizione (ad es., con la creazione di fondi a seguito di contratti stipulati a prezzi superiori a quelli di mercato o con l'assegnazione di contratti a persone o società gradite ai soggetti pubblici per ottenerne favori nell'ambito dello svolgimento di altre attività aziendali).

L'indebito beneficio, realizzato attraverso il processo d'acquisizione, è l'elemento costitutivo del reato in oggetto, da associare alla qualità di pubblico ufficiale o incaricato di pubblico servizio del soggetto passivo e all'atto d'ufficio da compiere, omettere o ritardare.

Il reato di riciclaggio potrebbe essere commesso in conseguenza della mancata verifica preventiva circa l'affidabilità delle controparti commerciali e/o dei partner operativi/finanziari in occasione delle stipulazione di accordi (ATI/RTI) con altre imprese per la realizzazione dell'attività.

ATTIVITÀ DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e della **valutazione complessiva delle forniture**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di **attori diversi** operanti nelle seguenti fasi/attività del processo:
  - richiesta della fornitura,
  - effettuazione dell'acquisto,
  - certificazione dell'esecuzione dei servizi/consegna dei beni (rilascio benestare),
  - effettuazione del pagamento.
- Esistenza di criteri tecnico-economici per:

- la selezione di potenziali fornitori (Qualificazione e inserimento),
- la validazione della fornitura e dei beni/servizi forniti,
- la valutazione complessiva dei fornitori.

- Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili).
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati prevedendo una specifica clausola che vincoli i fornitori al rispetto dei principi etico-comportamentali adottati dalla Società e, per servizi in *outsourcing* , la facoltà della Società di condurre attività di audit presso il prestatore del servizio al fine di verificare il rispetto degli obblighi contrattuali.
- Esistenza di livelli di approvazione per la formulazione delle richieste di acquisto e per la certificazione della fornitura/erogazione e di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni.
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

Devono, inoltre, essere definite modalità di escalation autorizzativa per le attività d'acquisizione gestite in deroga ai requisiti sopra esposti (ad es., per scelta di fornitori non presenti in Albo, mancata comparazione fra offerte alternative, ecc.).

FLUSSI INFORMATIVI VERSO ORGANISMO DI VIGILANZA

Il Responsabile degli Acquisti deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: Elenco degli acquisti effettuati in deroga ai requisiti sopra indicati.

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "B"

Aree di attività nel cui ambito possono essere commessi i reati societari ex artt. 25 ter e sexies del D. Lgs. 231/2001

B.E.E. Team spa *–Tutti i diritti riservati.*

1. FUNZIONE DELLA PARTE SPECIALE

La Parte Speciale B tratta i reati societari e di market abuse di cui agli artt. 25 ter.

Obiettivo della presente disciplina è che tutti i soggetti interessati tengano comportamenti conformi a quanto prescritto nel Modello, al fine di prevenire la commissione dei reati societari richiamati dal D. Lgs. 231/01.

2. TIPOLOGIA DEI REATI SOCIETARI E DI MARKET ABUSE

Si riporta, di seguito, l'elenco dei principali reati societari contemplati dal D. Lgs. 231/01 la cui commissione possa, comunque, comportare un beneficio da parte della Società:

a. False comunicazioni sociali e false comunicazioni sociali in danno dei soci e dei creditori (artt. 2621 e 2622 c.c)
b. Falso in prospetto (art.173-bis T.U.F)
c. Impedito controllo (art. 2625 c.c.) (modificato dall'art. 37 del D.Lgs. 27 gennaio 2010, n. 39)
d. Illecite operazioni sulle azioni o quote sociali proprie o della società controllante (art. 2628 c.c.)
e. Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
f. Indebita restituzione dei conferimenti (art. 2626 c.c.)
g. Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)
h. Formazione fittizia del capitale (art. 2632 c.c.)
i. Illecita influenza sull'Assemblea (art. 2636 c.c.)
j. Abuso di informazioni privilegiate (art. 184 e art. 187-*bis* T.U.F.)
k. Aggiotaggio (art. 2637 c.c.)
l. Manipolazione del mercato (art. 185 e art. 187-*ter* T.U.F.)
m. Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale (art. 27, D.Lgs. 27.01.2010, n. 39)

3. PROCESSI SENSIBILI NELL'AMBITO DEI REATI SOCIETARI E DI MARKET ABUSE

I principali Processi Sensibili che B.E.E. TEAM Spa ha individuato al proprio interno sono i seguenti:

1. predisposizione delle comunicazioni ai soci relative alla situazione economica, patrimoniale e finanziaria della Società (bilancio d'esercizio e relazioni periodiche), e prospetti informativi a fronte di operazioni straordinarie (fusione, scissione, ecc.) e particolari;
2. predisposizione delle informazioni relative alla formazione del bilancio e delle relazioni periodiche a livello consolidato di Gruppo;

B.E.E. Team spa *–Tutti i diritti riservati.*

3. gestione e comunicazione di notizie/dati verso l'esterno nell'ambito di una strategia complessiva di comunicazione (rapporti con investitori istituzionali, comunicati price sensitive, rapporti con le Autorità di Vigilanza, ecc.);
4. operazioni relative al capitale sociale;

I processi sopra individuati, esposti al rischio di commissione dei reati societari di cui si tratta nella presente Parte Speciale, possono altresì dare luogo, sempre in relazione alle medesime fattispecie di reato, anche ai delitti di criminalità organizzata. Ne deriva che i protocolli di prevenzione e controllo, nel seguito indicati, costituiscono un presidio di contrasto anche in riferimento ai reati associativi, oltre agli specifici principi di carattere generale di cui alla Parte Speciale F.

4. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono gli amministratori e i sindaci (soggetti apicali) di B.E.E. TEAM Spa, nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, qui di seguito tutti denominati "Destinatari".

Per quanto concerne gli amministratori ed i sindaci, la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto". Ai sensi dell'art. 2639 C.C., infatti, dei reati societari previsti dal Codice Civile risponde sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo i poteri tipici inerenti alla qualifica o alla funzione.

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di prevenire la commissione dei reati previsti dal Decreto.

5. REGOLE GENERALI

5.1 Il sistema in linea generale

Nello svolgimento delle operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli Organi Sociali di B.E.E. TEAM Spa e più in generale i "Destinatari" della presente Parte Speciale devono conoscere e sono tenuti a rispettare:

a) il Codice Etico di B.E.E. TEAM Spa;
b) il sistema di controllo interno, le procedure/linee guida aziendali e il sistema di controllo della gestione;
c) la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa (organigrammi);
d) i principi contabili nazionali ed internazionali;

e) il sistema disciplinare di cui al CCNL;
f) in generale, la normativa italiana e straniera applicabile;
g) le leggi, norme e regolamenti, per quanto applicabili, emanati dagli enti di controllo dei mercati.

Tutte le informazioni aventi natura privilegiata devono essere comunicate in modo tale che l'eventuale diffusione avvenga esclusivamente tramite i canali a ciò espressamente deputati.

5.2 Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico dei "Destinatari" di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate (art. 25-ter e sexies del D. Lgs. 231/01);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate, possano potenzialmente diventarlo;
- violare i principi e le procedure aziendali previste dalla presente Parte Speciale.

Conseguentemente i soggetti sopra indicati hanno l'espresso obbligo di:

1. Tenere un comportamento corretto e trasparente, conforme alle norme di legge ed alle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, in modo che ai soci ed ai terzi venga fornita un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società e del Gruppo.
   In particolare, è fatto divieto di:
   - rappresentare o trasmettere per l'elaborazione e la rilevazione in bilanci, relazioni, prospetti o altre comunicazioni sociali, dati difformi dal vero o incompleti sulla situazione economica, patrimoniale e finanziaria della Società e del Gruppo;
   - omettere dati od informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società e del Gruppo.

2. Osservare la normativa di legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere.
   In particolare, è fatto divieto di:
   a) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

b) ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserve legali non distribuibili;
c) acquistare o sottoscrivere azioni della società o di società controllate fuori dai casi previsti dalla legge;
d) effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
e) procedere alla formazione od all'aumento fittizi del capitale sociale;
f) distrarre i beni sociali, in sede di liquidazione della società, dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli.

3. Assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo e rendendo agevole e trasparente ogni forma di controllo interno sulla gestione sociale, nonché la libera e corretta formazione della volontà assembleare.
   In particolare, è fatto divieto di:
   a) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte dei soci, del Collegio Sindacale o della Società di Revisione;
   b) determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, compiendo atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assemblare.
4. Tenere comportamenti rispettosi delle norme di legge e delle procedure interne, assicurando la massima accuratezza nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni relative agli strumenti finanziari emessi o garantiti dalla società, necessari per permettere agli investitori di formarsi un giudizio correttamente basato in ordine alla situazione patrimoniale, economica e finanziaria della società, all'evoluzione della sua attività, nonché ai suoi strumenti finanziari e relativi diritti.
   In particolare è fatto divieto di:
   a. modificare in qualunque modo dati o informazioni destinati alla redazione dei prospetti informativi;
   b. illustrare dati e informazioni in modo fuorviante, tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società ovvero sull'evoluzione dell'attività sociale, nonché sugli strumenti finanziari e relativi diritti;

5. Evitare di porre in essere operazioni simulate o diffondere notizie difformi dal vero idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari.

In particolare è fatto divieto di pubblicare o divulgare notizie difformi dal vero o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio, aventi ad oggetto strumenti finanziari quotati o non quotati, idonei ad alterarne sensibilmente il prezzo;

6.Effettuare con tempestività, correttezza e completezza ogni comunicazione prevista dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, senza interporre ostacolo alcuno all'esercizio delle funzioni di vigilanza esercitate da tali autorità.

In particolare è fatto divieto di:

a. omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche, previste dalle leggi e dalla normativa applicabile, nei confronti delle autorità di vigilanza cui è soggetta l'attività della società, nonché omettere la trasmissione dei dati e dei documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;

b. esporre nelle comunicazioni di qualunque genere fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;

c. porre in essere qualsiasi comportamento di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche di vigilanza.

6. DOCUMENTI DIFFUSI TRA GLI ORGANI SOCIALI DI B.E.E. TEAM Spa.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli Organi Sociali di B.E.E. TEAM Spa devono in generale conoscere e rispettare:

a) il Codice Etico di B.E.E. TEAM Spa;
b) il sistema di controllo interno, nonché le procedure aziendali e il sistema di controllo della gestione che lo compongono;
c) la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa (organigrammi);
d) le procedure della società;
e) il sistema disciplinare di cui al presente M.O.;
f) in generale, la normativa italiana applicabile.

7. PROCEDURE E CONTROLLI SPECIFICI

Di seguito vengono indicate le procedure ed i controlli previsti a livello delle specifiche tipologie di reato di cui all'art. 25-ter e sexies del Decreto, con evidenza, per ciascuna di esse:

- dei processi aziendali sensibili;

- delle procedure e i controlli previsti dalla Società per prevenire la commissione dei reati di cui si tratta.

In linea generale, ai fini della prevenzione dei reati societari e di market abuse, oltre a quanto nel seguito indicato, devono essere previsti dei programmi di informazione e formazione rivolta

- a tutti i responsabili delle funzioni coinvolte nella redazione del bilancio e delle altre comunicazioni sociali, in merito alle principali nozioni e problematiche giuridiche e contabili sul bilancio ed alle loro evoluzioni;
- agli amministratori, al management ed ai dipendenti, sulle regole di Corporate Governance e sui reati o illeciti amministrativi in materia societaria.

7.1 False comunicazioni sociali e false comunicazioni sociali in danno degli azionisti e dei creditori (artt. 2621 e 2622 c.c)

Aree a rischio

- Amministrazione
- Gestione della Finanza
- Vertice Aziendale.

Descrizione della fattispecie

- Si tratta di due ipotesi criminose (la prima una contravvenzione e la seconda un delitto) la cui condotta tipica coincide quasi totalmente e che si differenziano per il verificarsi o meno di un danno patrimoniale ai soci o ai creditori della Società.
- Le due fattispecie criminose si realizzano tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori ed il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.
- Il reato può essere commesso nell'interesse della società nel caso, ad esempio, di creazione di riserve occulte illiquide, ottenute attraverso la sottovalutazione di poste attive o la sopravvalutazione di quelle passive per favorire l'autofinanziamento dell'impresa sociale ovvero coprire eventuali perdite intervenute nell'esercizio sociale.
- Soggetti attivi del reato sono gli Amministratori, i Direttori Generali, i Sindaci.

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.

- Predisposizione dei documenti di cui si tratta (bilanci, relazioni o altre comunicazioni sociali previste dalla legge, diretti ai soci o al pubblico) in base a specifiche procedure che:
  - assicurino la precisione e la completezza dei dati e delle notizie che ogni funzione interessata deve fornire nonché il rispetto e l'adeguatezza dei criteri contabili per l'elaborazione dei dati stessi, prevedendo la definizione delle funzioni coinvolte, delle scadenze da osservare, degli argomenti oggetto di comunicazione e informativa, nonché l'organizzazione dei relativi flussi;
  - regolino la trasmissione di dati e informazioni alla funzione responsabile attraverso un sistema (anche informatico) che garantisce la documentazione dei singoli passaggi nonché l'identificazione dei soggetti che inseriscono i dati;
  - regolino criteri e modalità per l'elaborazione dei dati del bilancio consolidato e la trasmissione degli stessi da parte delle società rientranti nel perimetro di consolidamento.
- Tempestiva messa a disposizione a tutti i membri del CdA, della bozza del bilancio e della relazione della società di revisione, predisponendo idonea documentazione dell'avvenuta consegna di tali documenti.
- Sottoscrizione da parte del massimo vertice esecutivo della cosiddetta lettera di attestazione o manleva richiesta dalla società di revisione.
- Prassi di riunioni di coordinamento tra i diversi organi di controllo.
- Comunicazione sistematica all'Organismo di Vigilanza di qualsiasi incarico conferito, o che si intende conferire, alla società di revisione o a società ad essa collegate, diverso da quello concernente la certificazione di bilancio.
- Invio all'Organismo di Vigilanza delle valutazioni in ordine alla scelta della società di revisione.

7.2 Falso in prospetto (art.173-bis T.U.F)

Aree a rischio

- Amministrazione
- Gestione della Finanza
- Vertice Aziendale.

Descrizione della fattispecie

- L'art. 34 della Legge n. 262 del 2005 (c.d. legge sul risparmio) ha introdotto il nuovo reato
- di falso in prospetto (inserendolo all'art. 173-bis del TUF), disponendo contestualmente l'abrogazione dell'art. 2623 c.c.
- Poiché l'art. 25-ter, lett. c) e d) fa espresso richiamo all'art. 2623 c.c. quale presupposto
- dell'illecito amministrativo, l'abrogazione della norma del codice civile, cui non si accompagna l'integrazione dell'art. 25-ter con il riferimento alla nuova fattispecie dell'art. 173-bis TUF, dovrebbe determinare, quale conseguenza, la non applicabilità della sanzione amministrativa ai sensi del Decreto al nuovo reato di falso in prospetto.
- La mancanza di precedenti giurisprudenziali sul punto induce tuttavia, in un'ottica prudenziale, a tener conto anche di tale fattispecie.
- La condotta illecita consiste nell'esporre false informazioni o nell'occultare dati e notizie, in modo da indurre in errore i destinatari dei prospetti informativi richiesti per la sollecitazione all'investimento o l'ammissione alla quotazione nei mercati regolamentati o in occasione delle offerte pubbliche di acquisto e di scambio.
- Relativamente all'elemento oggettivo del reato, si osserva che esso può oggi risultare integrato in entrambe le ipotesi – delittuosa e contravvenzionale – sia da una condotta commissiva (esposizione di false informazioni) che da una condotta omissiva (occultamento di dati o notizie, la cui natura non è peraltro in alcun modo specificata dalla legge), richiedendosi per entrambe l'idoneità a indurre in errore i destinatari del prospetto.

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.
- Al fine di prevenire la commissione del reato, sono stabilite regole/procedure interne che prevedono:
  a) Modalità di verifica della correttezza dei dati e delle informazioni di fonte interna e citazione della fonte per quelle provenienti dall'esterno dell'Azienda.
  b) Impiego di informazioni previsionali dalle funzioni ed approvate dal CdA e/o dall'Amministratore Delegato.
  c) Individuazione di un soggetto responsabile per ogni singola operazione di redazione di prospetti informativi.

d) Diffusione dei principi di comportamento in materia previsti dal presente Modello nel contesto dell'intera organizzazione aziendale, in modo che gli amministratori, il management e tutti i dipendenti possano fornire agli organi di controllo la massima collaborazione e correttezza.

e) Predisposizione di meccanismi sanzionatori interni nei confronti di quei soggetti dell'organizzazione che non abbiano rispettato le norme di cui sopra.

f) Informativa all'Organismo di Vigilanza da parte del soggetto responsabile dell'operazione di ciascuna iniziativa che richieda la redazione di prospetti e della loro avvenuta pubblicazione.

- Verifica di coerenza del sistema di deleghe e procure anche in tema di disciplina di Corporate Governance.

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

Aree a rischio

- Amministrazione
- Gestione della Finanza
- Vertice Aziendale.

Procedure e controlli

Stante la particolare natura della fattispecie, i controlli ipotizzabili sono quelli indicati per la prevenzione del reato in false comunicazioni sociali.

7.4 Impedito controllo (art. 2625 c.c.) (modificato dall'art. 37 del D.Lgs. 27 gennaio 2010, n. 39)

Aree a rischio

- Amministrazione
- Gestione della Finanza
- Vertice Aziendale.

Descrizione della fattispecie

- La condotta consiste nell'impedire od ostacolare, mediante occultamento di documenti o altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alla Società di Revisione.

- A titolo di esempio, gli Amministratori, anche avvalendosi di propri diretti collaboratori, non forniscono ad un membro del Collegio Sindacale i documenti da questo richiesti nell'esercizio delle proprie attività di controllo

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.
- Al fine di prevenire la commissione del reato, sono stabilite le seguenti regole/procedure interne:
  a) trasmissione al Collegio Sindacale di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'Assemblea o del CdA o sui quali esso debba esprimere un parere ai sensi di legge;
  b) messa a disposizione degli organi di controllo (Collegio Sindacale, Società di revisione, Comitato di Controllo) di tutta la documentazione di cui essi necessitino per lo svolgimento dei loro controlli;
  c) diffusione dei principi di comportamento in materia previsti dal presente Modello nel contesto dell'intera organizzazione aziendale, in modo che gli amministratori, il management e tutti i dipendenti possano fornire agli organi di controllo la massima collaborazione e correttezza;
  d) predisposizione di meccanismi sanzionatori interni nei confronti di quei soggetti dell'organizzazione che non abbiano rispettato le norme di cui sopra.
- Verifica di coerenza del sistema di deleghe e procure anche in tema di disciplina di Corporate Governance.

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

Aree a rischi

- Vertice Aziendale.

Descrizione della fattispecie

- La fattispecie punisce gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, ovvero, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge. La legge prevede poi una causa di esclusione della punibilità nel caso in cui il capitale sociale o le riserve siano ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è

stata posta in essere la condotta. La norma mira a tutelare l'integrità e l'effettività del capitale sociale e delle riserve non distribuibili per legge, rispetto a fenomeni di annacquamento del medesimo che potrebbero pregiudicare l'interesse dei creditori.

- Il reato può essere commesso dagli Amministratori.

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.
- Formalizzazione delle procedure per l'acquisto sia di azioni proprie B.E.E. Team sia di partecipazioni nelle società controllanti da parte di società del Gruppo (l'acquisto di tali partecipazioni deve sempre avvenire nei limiti previsti dal Codice Civile e dallo Statuto).
- Predisposizione di meccanismi sanzionatori interni nei confronti di quei soggetti dell'organizzazione che non abbiano rispettato le norme di cui sopra.
- Verifica dell'attuale sistema di deleghe e procure coerenti anche in tema di disciplina di Corporate Governance.

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

Aree a rischio

- Vertice Aziendale.

Descrizione della fattispecie

- La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Con riferimento alle operazioni di riduzione del capitale sociale, si porta quale esempio di condotta penalmente rilevante l'esecuzione della delibera di riduzione del capitale sociale nonostante l'opposizione dei creditori sociali o in mancanza della delibera da parte del Tribunale. Con riferimento alle operazioni di fusione o di scissione, si può ricordare l'esecuzione di dette operazioni prima del termine di cui all'art. 2503 comma 1, ove non ricorrano le eccezioni ivi previste ovvero in presenza di opposizione e senza l'autorizzazione del Tribunale.
  - Soggetti attivi del reato sono gli Amministratori.

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti del Codice Etico della Società.

- Prevedere che le operazioni straordinarie avvengano sempre nel rispetto delle norme fissate dal Codice Civile.
- Predisposizione di meccanismi sanzionatori interni nei confronti di quei soggetti dell'organizzazione che non abbiano rispettato le norme di cui sopra.
- Verifica di coerenza del sistema di deleghe e procure anche in tema di disciplina di Corporate Governance.

7.7 Indebita restituzione dei conferimenti (art. 2626 c.c.) e illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

Aree a rischio

- Vertice Aziendale.

Descrizione della fattispecie

Indebita restituzione dei conferimenti

Il reato si integra attraverso la restituzione dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli, in maniera palese o simulata, fuori dei casi di legittima riduzione del capitale sociale.

Soggetti attivi del reato sono gli Amministratori, resta tuttavia la possibilità del concorso, secondo le regole generali di cui agli artt. 110 e seguenti del c.p., dei Soci che hanno svolto un'attività di istigazione o di ausilio nei confronti degli Amministratori.

Illegale ripartizione degli utili o delle riserve

La condotta criminosa di tale reato, di natura contravvenzionale, consiste nel ripartire gli utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Si fa presente che la ricostituzione degli utili o delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti del Codice Etico della Società.
- Preciso richiamo al rispetto della legge e delle norme statutarie nelle restituzioni di conferimento e nelle distribuzioni di utili o riserve.
- Pronta comunicazione ai creditori delle operazioni suddette, nel caso in cui portino a riduzioni del capitale sociale, al fine di ottenere la loro autorizzazione, secondo quanto previsto dalle norme del Codice Civile.

B.E.E. Team spa *–Tutti i diritti riservati.*

- Predisposizione di meccanismi sanzionatori interni nei confronti di quei soggetti dell'organizzazione che non abbiano rispettato le norme di cui sopra.
- Verifica di coerenza del sistema di deleghe e procure anche in tema di disciplina di Corporate Governance.

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

Aree a rischio

- Amministrazione.
- Gestione della Finanza.
- Vertice Aziendale.

Descrizione della fattispecie

Tale ipotesi di reato è integrata dalle seguenti condotte:

- formazione o aumento fittizio del capitale della società mediante attribuzione di azioni o quote sociali per una somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura, dei crediti ovvero del patrimonio della società, nel caso di trasformazione.

Soggetti attivi di questa fattispecie possono essere gli Amministratori *e* i Soci conferenti.

Procedure e controlli

- Diffusione tra i soggetti apicali e i dipendenti del Codice Etico della Società.
- Preciso richiamo al rispetto della legge e delle norme statutarie nello svolgimento delle operazioni di formazione ed incremento del capitale sociale.
- Predisposizione di meccanismi sanzionatori interni nei confronti di quei soggetti dell'organizzazione che non abbiano rispettato le norme di cui sopra.
- Verifica di coerenza del sistema di deleghe e procure anche in tema di disciplina di Corporate Governance.

7.9 Illecita influenza sull'Assemblea (art. 2636 c.c.)

Aree a rischio

- Vertice Aziendale.

Descrizione della fattispecie

Il reato si attua quando, con atti simulati o con frode, si determina la maggioranza in Assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

È opportuno ricordare che la responsabilità dell'ente è configurabile solo quando la condotta prevista dall'articolo in esame sia realizzata nell'interesse dell'Ente. Ciò rende difficilmente ipotizzabile il reato in questione che, di norma, viene realizzato per favorire interessi di parte e non dell'ente.

L'ipotesi di reato è integrata, a titolo di esempio, dalla seguente condotta: L'Amministratore delegato, anche avvalendosi dei suoi collaboratori, provvede a presentare all'Assemblea, in relazione ad un determinato ordine del giorno, atti e documenti falsi o non completi comunque alterati in alcuni loro contenuti, allo scopo di indurre l'Assemblea ad approvare una puntuale delibera su uno specifico argomento,

Il reato può essere commesso da chiunque ("reato comune"), quindi anche da soggetti esterni alla società.

Procedure e controlli:

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.
- Presenza di norme statutarie che disciplinano le modalità di partecipazione e di svolgimento delle assemblee sociali, nonché le maggioranze previste per l'adozione delle delibere assembleari.

7.10 Abuso di informazioni privilegiate (art. 184 T.U.F.)

Aree a rischio:

- Vertice Aziendale.
- Organi amministrativi.
- Management e dipendenti operanti nelle attività a rischio.

Descrizione della fattispecie

Si determina l'illecito qualora che un soggetto in posizione apicale o un sottoposto utilizzi informazioni di cui è entrato in possesso (lecitamente o illecitamente) per realizzare operazioni sugli strumenti finanziari emessi dalla società Capogruppo o da altre società del Gruppo, in particolare:

- acquisto, vendita o altre operazioni (direttamente o indirettamente)
- comunicazione delle informazioni ad altri soggetti al di fuori dell'ordinario esercizio dell'attività lavorativa

B.E.E. Team spa *–Tutti i diritti riservati.*

- raccomandazione ad altri o induzione di altri soggetti ad acquistare, vendere o compiere altre operazioni.

Procedure e controlli:

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.
- Introduzione del divieto di compimento di operazioni personali, per conto proprio o di terzi, effettuate utilizzando informazioni privilegiate, relative alla Società ed al Gruppo di appartenenza, acquisite in ragione delle proprie funzioni.
- Al fine di prevenire la commissione del reato a livello di Società e/o di Gruppo, sono stabilite regole/procedure interne relative a:
  - gestione, diffusione, trattamento e modalità di protezione delle informazioni privilegiate anche attraverso l'introduzione di meccanismi di tracciabilità degli accessi;
  - definizione dei criteri per l'individuazione delle informazioni privilegiate e le condizioni per la loro eventuale comunicazione a terzi;
  - presidi procedurali volti a garantire che la circolazione delle informazioni privilegiate nell'ambito della Società avvenga nel rispetto del principio della oggettiva necessità di comunicazione in relazione all'attività svolta (c.d. "need to know");
  - informativa ai soggetti rilevanti in merito agli obblighi giuridici e regolamentari che derivano dall'aver accesso alle informazioni privilegiate;
  - modalità di formazione e diffusione delle notizie relative alla società e individuazione dei soggetti cui compete il controllo sulla correttezza e diffondibilità delle informazioni.

7.11 Manipolazione del mercato (art. 185 T.U.F.)

Aree a rischio:

- Vertice Aziendale.
- Organi amministrativi.
- Management.

Descrizione della fattispecie

L'abuso di mercato realizzato attraverso l'alterazione delle dinamiche relative alla corretta

formazione del prezzo di strumenti finanziari viene oggi punito, sia come reato, dagli artt. 2637 c.c. (aggiotaggio) e 185 TUF (manipolazione del mercato) sia da un illecito amministrativo, previsto dall'art. 187-ter TUF.

Le due ipotesi di reato si distinguono in relazione alla natura degli strumenti finanziari il cui

prezzo potrebbe essere influenzato dalle condotte punite. Nel caso dell'aggiotaggio, vengono presi in considerazione strumenti finanziari non quotati o per i quali non sia stata presentata domanda di ammissione alla negoziazione in un mercato regolamentato; nel caso del reato e dell'illecito amministrativo di manipolazione del mercato, si tratta di strumenti finanziari quotati per i quali sia stata presentata richiesta di ammissione alla negoziazione su mercati regolamentati.

Il reato si attua con la diffusione, con qualsiasi mezzo (incluso Internet), di informazioni, voci, o notizie fuorvianti o false che possano potenzialmente fornire indicazioni distorcenti in merito agli strumenti finanziari; la fattispecie si configura anche in presenza di operazioni (ordini di compravendita) che diano o possano dare informazioni egualmente distorcenti o che portino a fissare prezzi di mercato a livelli anomali.

Procedure e controlli:

- Diffusione tra i soggetti apicali e i dipendenti di B.E.E. TEAM Spa del Codice Etico della Società.
- Introduzione del divieto di compimento di operazioni personali, per conto proprio o di terzi, effettuate utilizzando informazioni privilegiate acquisite in ragione delle proprie funzioni;
- Introduzione del divieto di diffondere informazioni comunque fuorvianti relative a strumenti finanziari o ad altre circostanze che possano anche solo potenzialmente influire sul prezzo degli strumenti finanziari stessi.

Al fine di prevenire la commissione del reato, a livello di Società e/o di Gruppo, sono stabilite regole/procedure interne relative a:

- comportamento degli esponenti aziendali che abbiano accesso a informazioni privilegiate, con particolare riferimento agli obblighi informativi e di comportamento inerenti eventuali operazioni su strumenti finanziari;
- modalità di formazione e diffusione delle notizie relative alla società e individuazione dei soggetti cui compete il controllo sulla correttezza e diffondibilità delle informazioni;
- le operazioni su titoli della Società con previsione di espresso divieto di operare al di fuori di programmi autorizzati;

- la previsione di specifiche cautele contrattuali, volte a regolare il trattamento e l'accesso ad informazioni privilegiate da parte di consulenti/partner (previsione di clausole di riservatezza).

8. FLUSSI VERSO L'ORGANISMO DI VIGILANZA

Sono previsti flussi informativi tra gli organi di controllo (Collegio Sindacale, Società di Revisione, Comitato di Controllo) e quelli di gestione (CdA, Amministratore Delegato, Presidente) della Società (riunioni), anche per verificare l'osservanza della disciplina prevista in tema di materia societaria e regole di Corporate Governance. modifiche di Bilancio richieste in sede di approvazione dal C.d.A.; in particolare le:

- anomalie emerse in sede di effettuazione delle verifiche sui dati di chiusura e sull'applicazione dei controlli amministrativo-contabili;
- anomalie rilevate/segnalate dalla Società di Revisione o dal Collegio Sindacale nello svolgimento delle rispettive attività di verifica.

Vengono segnalati all'Organismo di Vigilanza gli eventuali casi di irregolarità riscontrate nel corso delle attività di controllo.

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "C"

Reati di omicidio colposo e di lesioni colpose gravi e gravissime in violazione degli adempimenti in materia di tutela della salute e della sicurezza sul lavoro. (Art . 25 septies D. Lgs. 231/01)

B.E.E. Team spa *–Tutti i diritti riservati.*

1. FUNZIONI DELLA PARTE SPECIALE

La Parte Speciale C ha come obiettivo la disciplina dei comportamenti finalizzati a prevenire la commissione dei reati previsti all'art 25 septies del D. Lgs. 231, mediante l'attuazione di un "*sistema aziendale per l'adempimento di tutti gli obblighi*" di cui all'art. 30 del dal Testo Unico sulla Sicurezza (T.U.S.: Decreto Legislativo n. 81 del 9 aprile 2008 e seguenti) basato su;

- la definizione di una politica aziendale per la sicurezza,
- l'analisi dei rischi,
- la definizione di procedure ed istruzioni comportamentali,
- la formazione e l'addestramento del personale,
- l'auto-controllo (ispezioni interne),
- la registrazione formalizzata delle attività svolte,
- il riesame periodico degli obiettivi di miglioramento da parte del vertice aziendale.

Alle violazioni delle normative in materia di tutela della salute e sicurezza sul lavoro, di cui si tratta nella presente Parte Speciale, possono altresì accompagnarsi anche i delitti di criminalità organizzata.
Ne deriva che i protocolli di prevenzione e controllo, nel seguito indicati, costituiscono un presidio di contrasto anche in riferimento ai reati c.d. associativi, oltre agli specifici principi e regole di cui alla Parte Speciale F.

2. DESTINATARI DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i "Destinatari").
Obiettivo della presente Parte Speciale è che tutti i Destinatari siano consapevoli della valenza dei comportamenti tenuti e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

3. AREE DI ATTIVITA' A RISCHIO

Per la individuazione delle aree di attività nel cui ambito possono essere commessi i reati sopra richiamati, si deve fare riferimento a quanto definito nel Documento di Valutazione dei Rischi (DVR) redatto in ottemperanza agli obblighi di cui al D.Lgs 81/2008.

4. REGOLE GENERALI

4.1 Il sistema in linea generale

La presente sezione del Modello è rivolta ai soggetti aziendali che si trovano in condizioni tali da doverla applicare e/o rispettare, nello svolgimento di Attività a Rischio, al fine di prevenire

comportamenti idonei al verificarsi dei reati di cui all'art. 25 *septies* del D. Lgs. 231/01. Tutto ciò con obblighi differenziati in relazione al ruolo ed alle responsabilità loro assegnati in azienda, con particolare riferimento a:

- **Datore di Lavoro**
- **Dirigenti**
- **Appaltatori**
- **Preposti**
- **Medico competente**
- **Dipendenti**
- **Organismo di Vigilanza**

Nello svolgimento delle operazioni attinenti le Attività a Rischio dei reati di cui si tratta, oltre alle regole previste dal presente Modello, i Destinatari di questo Sistema, sono tenuti a rispettare:

4. normativa italiana e straniera applicabile;
5. il Codice Etico;
6. il sistema di controllo interno (le procedure/linee guida aziendali, la documentazione e le disposizioni regolanti la materia in questione);
7. i principi contabili nazionali e internazionali inerenti ai costi della sicurezza nei contratti di somministrazione di appalto e subappalto nel ramo dei pubblici appalti.

Il sistema posto in atto dalla Società per la prevenzione dei reati di cui si tratta, in coerenza con la normativa vigente in materia, prevede l'adozione delle seguenti misure:

4.1.1 Requisiti e competenze

α. Nomina formale del Responsabile Servizio di Prevenzione e Protezione (R.S.P.P.), del Medico competente, degli addetti al primo soccorso, alla prevenzione incendi e alla gestione emergenza.

β. Individuazione dei soggetti tenuti a controllare l'attuazione delle misure di mantenimento-miglioramento.

χ. Il Responsabile e gli Addetti del Servizio di Prevenzione e Protezione (RSPP) ed il Medico competente devono avere capacità e requisiti professionali in materia di Prevenzione e Protezione.

δ. Il Medico competente deve partecipare all'organizzazione della valutazione dei rischi, delle attività di tutela e dei monitoraggi ambientali e ricevere copia dei risultati.

4.1.2 Informazione

a. Attività di informazione a dipendenti e nuovi assunti sui rischi specifici dell'impresa.

b. Evidenza dell'informativa erogata in materia di sicurezza e verbalizzazione degli incontri.
c. Documentazione formale dell'informazione e delle istruzioni per l'uso delle attrezzature di lavoro.
d. Organizzazione di incontri periodici tra le funzioni preposte alla sicurezza sul lavoro.
e. Informazione sulla nomina del Responsabile del Servizio di Prevenzione e Protezione (RSPP), sul Medico competente e sugli addetti ai compiti specifici.
f. Coinvolgimento del Responsabile SPP e/o del Medico nella definizione delle informazioni.
g. Coinvolgimento dei Rappresentante dei Lavoratori per la Sicurezza (RLS) nella organizzazione della attività di rilevazione e valutazione dei rischi e nella designazione degli addetti.

4.1.3 Formazione

α. Formazione a tutti i dipendenti in materia di sicurezza sul lavoro.

β. Somministrazione di questionari di valutazione.

χ. Verifica dell'adeguatezza della formazione ai rischi della mansione cui il lavoratore è in concreto assegnato.

δ. Predisposizione di uno specifico piano di formazione per i lavoratori esposti a rischi gravi ed immediati.

ε. Formazione preventiva, aggiuntiva e specifica, per i lavoratori che cambiano mansione e per quelli trasferiti.

ϕ. Partecipazione del Servizio di Prevenzione e Protezione (RSPP) e/o del Medico competente alla stesura del piano di formazione.

γ. Specifica formazione per gli addetti a specifici compiti in materia di prevenzione e protezione.

η. Periodiche esercitazioni di evacuazione con relativa verbalizzazione.

4.1.4 Registri ed altri documenti

α. Aggiornamento del registro infortuni e del registro delle pratiche delle malattie professionali.

β. Predisposizione del registro degli esposti agli agenti cancerogeni e mutageni.

B.E.E. Team spa *–Tutti i diritti riservati.*

χ. Evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente tra il Responsabile del Servizio di Prevenzione e Protezione (RSPP) ed il Medico competente.

δ. Tenuta di un archivio degli adempimenti in materia di sicurezza e igiene sul lavoro.

ε. Il documento di valutazione dei rischi deve indicare gli strumenti ed i metodi con i quali si è proceduto alla valutazione e contenere il programma delle misure di mantenimento e miglioramento.

4.1.5 Riunioni

Incontri periodici tra le funzioni preposte, in cui sia consentita la partecipazione all'Organismo di Vigilanza/Comitato di Controllo, organizzati con formale convocazione e relativa verbalizzazione.

4.2 Principi generali di comportamento

E' fatto espresso divieto a coloro che, per attività o funzione svolta, si trovano nella condizione di applicare e osservare la normativa in tema di sicurezza sotto ogni profilo, di porre in essere, ovvero dare causa a condotte che integrino, direttamente o indirettamente, i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi in violazione delle norme antinfortunistiche in materia di tutela della salute e della sicurezza sul lavoro.
In relazione a tutto quanto precede e tenuto conto della loro specifica posizione aziendale (ruolo e responsabilità) i soggetti come sopra individuati sono tenuti ai seguenti obblighi:

Il Datore di lavoro deve:

Nomina dei responsabili:

- designare il Responsabile del Servizio di Prevenzione e Protezione (RSPP) interno all'azienda;

Valutazione dei rischi:

1. valutare i rischi per la sicurezza e per la salute dei lavoratori, compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, quelli legati all'utilizzo di attrezzature e materiali di lavoro, e quelli connessi ai luoghi di lavoro;

2. elaborare, all'esito di tale valutazione, un documento (da custodirsi presso l'azienda o l'unità produttiva) contenente:

- una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale sono specificati i criteri adottati per la valutazione stessa;

- l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi per la sicurezza e per la salute dei lavoratori;
- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione (RSPP) e con il Medico competente nei casi in cui sia obbligatoria la sorveglianza sanitaria, previa consultazione del Rappresentante dei Lavoratori per la Sicurezza (RLS), e va nuovamente effettuata in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei lavoratori.

Il Datore di lavoro ed i Dirigenti devono:

Nomina dei responsabili:

1. designare gli Addetti del Servizio di Prevenzione e Protezione (ASPP) interno o esterno all'azienda;
2. nominare il Medico competente;
3. designare i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei lavoratori in caso di pericolo grave e immediato, di pronto soccorso e, comunque, di gestione dell'emergenza;
4. affidare ai lavoratori compiti che tengano conto delle loro capacità e condizione di salute;

Valutazione dei rischi:

1. valutare i rischi per la sicurezza e per la salute dei lavoratori, compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, quelli legati all'utilizzo di attrezzature e materiali di lavoro, e quelli connessi ai luoghi di lavoro;
2. elaborare, all'esito di tale valutazione, un documento (da custodirsi presso l'azienda o l'unità produttiva) contenente:
   - una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella qu**a**le sono specificati i criteri adottati per la valutazione stessa;
   - l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi per la sicurezza e per la salute dei lavoratori;
   - il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
   - l'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il Responsabile del Servizio di Prevenzione e protezione (RSPP) e con il

Medico competente nei casi in cui sia obbligatoria la sorveglianza sanitaria, previa consultazione del Rappresentante dei lavoratori per la sicurezza (RLS), e va nuovamente effettuata in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei lavoratori;

3. organizzare incontri periodici tra le funzioni preposte alla sicurezza sul lavoro;
4. consultare il Rappresentante dei lavoratori per la sicurezza (RLS) in ordine: alla valutazione dei rischi, all'individuazione, programmazione, realizzazione e verifica della prevenzione nella Società, alla designazione degli addetti al servizio di prevenzione, all'attività di prevenzione incendi, al pronto soccorso, all'evacuazione dei lavoratori; all'organizzazione della formazione dei lavoratori incaricati di gestione delle emergenze.

Misure di prevenzione

1. adottare le misure necessarie per la sicurezza e la salute dei lavoratori, in particolare:
   - designando preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei lavoratori in caso di pericolo grave e immediato, di , di pronto soccorso e, comunque, di gestione dell'emergenza;
   - aggiornando le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza del lavoro, ovvero in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
2. fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, di concerto con il Responsabile del Servizio di Prevenzione e Protezione;
3. prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno;
4. adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei lavoratori, nonché per il caso di pericolo grave e immediato. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda, ovvero dell'unità produttiva, e al numero delle persone presenti
5. richiedere al medico competente l'osservanza degli obblighi previsti a suo carico dalle norme in materia di sicurezza sul lavoro.

Informazione:

1. consentire ai lavoratori di verificare, mediante il Rappresentante dei lavoratori per la sicurezza (RLS), l'applicazione delle misure di sicurezza e di protezione della salute ed al Rappresentante medesimo di accedere alle informazioni ed alla documentazione aziendale inerente alla valutazione dei rischi, alle misure di prevenzione relative, nonché a quelle inerenti alle sostanze ed ai preparati pericolosi, alle macchine, agli impianti, all'organizzazione ed agli ambienti di lavoro, agli infortuni ed alle malattie professionali;

B.E.E. Team spa *–Tutti i diritti riservati.*

2. **erogare attività di informazione ai dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) circa i rischi specifici dell'impresa, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;**
3. assicurare l'evidenza dell'informativa erogata per la gestione di pronto soccorso, emergenza, evacuazione e prevenzione incendi e la verbalizzazione degli eventuali incontri;
4. informare dipendenti e nuovi assunti (compresi interinali, stagisti e co.co.pro) sulla nomina del Responsabile e degli Addetti al Servizio di Prevenzione Protezione (RSPP e ASPP), del Medico competente e degli addetti ai compiti specifici per il pronto soccorso, , evacuazione e prevenzione;
5. informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione
6. produrre documentazione formale dell'informazione e delle istruzioni per l'uso delle attrezzature di lavoro messe a disposizione dei dipendenti;
7. coinvolgere il Responsabile del Servizio di Prevenzione e Protezione (RSPP) e/o il Medico competente nella definizione delle informazioni.

Formazione

1. erogare a tutti i dipendenti la formazione in materia di sicurezza sul lavoro;
2. ottenere la partecipazione del Responsabile del Servizio di Prevenzione e Protezione (RSPP) e/o del Medico competente alla stesura del piano di formazione;
3. somministrare i questionari di valutazione;
4. verificare l'adeguatezza della formazione ai rischi della mansione cui il lavoratore è in concreto assegnato;
5. predisporre uno specifico piano di formazione per i lavoratori esposti a rischi gravi ed immediati;
6. erogare una formazione preventiva, aggiuntiva e specifica, per i lavoratori che cambiano mansione e per quelli trasferiti;
7. erogare specifica formazione per gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso);
8. prevedere periodiche esercitazioni di evacuazione, di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze);
9. erogare formazione specifica per i Rappresentante dei Lavoratori per la Sicurezza (RLS).

Registri ed altri documenti:

1. tenere il registro nel quale siano annotati cronologicamente gli infortuni sul lavoro che comportano un'assenza dal lavoro di almeno un giorno;
2. predisporre e tenere il registro degli esposti nell'ipotesi di esposizione ad agenti cancerogeni o mutageni.

Riunioni

1. organizzare incontri periodici tra le funzioni preposte, cui sia consentita la partecipazione all'Organismo di Vigilanza/Comitato di Controllo, mediante formale convocazione degli incontri e relativa verbalizzazione sottoscritta dai partecipanti.

Nei contratti d'appalto

A. **il datore di lavoro committente (appaltante) e l'appaltatore devono** elaborare un documento unico di valutazione dei rischi da interferenze (DUVRI), nel quale siano indicate le misure adottate per eliminare i rischi medesimi. Tale documento deve essere allegato al contratto di appalto o d'opera;

B. **la Società, in qualità di appaltante deve:**

1. in presenza di subappaltatori definire le procedure di gestione e di coordinamento dei lavori in subappalto;
2. verificare, anche attraverso l'iscrizione alla camera di commercio, industria e artigianato, l'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare in appalto o contratto d'opera;
3. indicare, nei contratti di somministrazione, di appalto e di subappalto, i costi relativi alla sicurezza del lavoro. A tali dati possono accedere, su richiesta, il Rappresentante dei lavoratori per la sicurezza (RLS) e le organizzazioni sindacali dei lavoratori;
4. definire, nei contratti di appalto, la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto;
5. fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
6. predisporre e mantenere aggiornato l'elenco delle aziende che operano all'interno dei propri siti con contratto d'appalto;
7. formalizzare le modalità di gestione e di coordinamento dei lavori in appalto in contratti scritti, nei quali siano presenti espressi riferimenti agli adempimenti di cui all'art. 26 D. Lgs. 81/08, tra i quali, in capo al datore di lavoro, "la verifica dell'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto";

8. cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;

x. **la Società, in qualità di appaltatrice deve:**

1. predisporre e mantenere aggiornato l'elenco delle aziende presso le quali opera come appaltatrice;
2. richiedere alle società presso le quali opera come tale le informazioni circa i rischi specifici e le misure preventive da queste adottate.

I Preposti devono:

1. verificare che soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
2. richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e individuali e, in caso di persistenza della inosservanza, informare i loro superiori diretti;
3. adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
4. informare i lavoratori esposti a rischi gravi e immediati circa i rischi stessi e le disposizioni prese o da prendere in materia di protezione;
5. astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
6. segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro.
7. Frequentare gli appositi corsi di formazione erogati secondo quanto previsto dalla normativa in dalle norme in materia di sicurezza sul lavoro.

Il Medico competente deve:

1. custodire, presso l'azienda ovvero l'unità produttiva, la cartella sanitaria e di rischio del lavoratore sottoposto a sorveglianza sanitaria, con salvaguardia del segreto professionale; dovrà esserne consegnata copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne faccia richiesta;
2. collaborare con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, all'attività di formazione e informazione nei confronti dei lavoratori e all'organizzazione del servizio di primo soccorso;

3. programmare ed effettuare la sorveglianza sanitaria;
4. fornire informazioni ai lavoratori e, su richiesta, al Rappresentante dei lavoratori per la sicurezza (RLS), sul significato della sorveglianza sanitaria;
5. comunicare per iscritto i risultati anonimi collettivi della sorveglianza sanitaria effettuata;
6. visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa che stabilisce in base alla valutazione dei rischi.

I Lavoratori devono:

1. osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
2. segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dispositivi di cui ai precedenti punti nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia ai Rappresentante dei lavoratori per la sicurezza (RLS);
3. non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
4. non compiere di propria iniziativa operazioni né manovre che non siano di loro competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori;
5. utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze e i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
6. utilizzare in modo appropriato i dispositivi di protezione messi a disposizione;
7. sottoporsi ai controlli sanitari previsti;
8. contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

4.3 Attività dell'Organismo di Vigilanza

L'attività dell'Organismo di Vigilanza deve fare riferimento alla specifica storia dell'Ente ed alle sue caratteristiche peculiari (precedenti violazioni in materia, procedimenti penali, numero infortuni ed entità degli stessi, libro degli infortuni ecc.).

L'Organismo di Vigilanza deve verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà e la puntuale applicazione degli aspetti di seguito riportati a titolo esemplificativo:

1. *Valutazioni del rischio:*
   - Documento di Valutazione dei Rischi (DVR) e relativi aggiornamenti; in tale ambito:
     - valutazione rischi luoghi di lavoro;

- valutazione del rischio incendio;
- valutazione del rischio chimico;
- valutazione rischi attrezzature di lavoro;
- valutazione di esposizione al rumore;
- valutazione rischio amianto;
- valutazione rischio vibrazioni;
- valutazione rischio microclima;
- valutazione della movimentazione manuale dei carichi e dei rischi di patologie da sforzi ripetuti (Cumulative Trauma Disorders - CTD);
- valutazione del rischio relativo all'uso dei videoterminali;
- valutazione rischio agenti cancerogeni;
- valutazione rischi in quota;
- valutazione rischio stress lavoro-correlato;
- programma degli interventi per il miglioramento dei livelli di sicurezza.

2. *Adempimenti formali*:

   - verbale CdA recante la designazione del datore di Lavoro;
   - deleghe ed incarichi per l'attuazione delle attività di sicurezza;
   - nomina del Responsabile e degli Addetti del Servizio di Prevenzione e Protezione (RSPP e ASPP);
   - elezione dei Rappresentante dei Lavoratori per la Sicurezza (RLS);
   - designazione degli addetti alla prevenzione incendi, al primo soccorso ed alla gestione dell'emergenza;
   - verbali delle riunioni periodiche di prevenzione e protezione dai rischi e delle consultazioni dei Rappresentante dei Lavoratori per la Sicurezza (RLS);
   - documentazione di avvenuta consegna dei Dispositivi di Protezione Individuale (DPI).

3. *Prevenzioni incendi e gestione dell'emergenza:*

   - certificato di prevenzione incendi;
   - piano di emergenza ed evacuazione;
   - attestati formazione squadra antincendio, primo soccorso e gestione emergenze;
   - verbali prove e gestione delle emergenze;
   - registro delle verifiche e manutenzioni sulle attrezzature antincendio (*ex* D.P.R. 37/98).

4. *Attività di formazione:*

   - attestati e verbali di formazione del personale preposto;
   - verbali di informazione e formazione lavoratori;
   - documentazione relativa alla formazione di: RSPP, ASPP e RLS.

5. *Documentazione procedurale, in conformità a quanto previsto al successivo punto 2.4.*

6. *Gestione dei contratti d'appalto e di prestazione d'opera.*

7. *Sorveglianza sanitaria:*

- nomina Medico competente;
- protocollo sanitario ed accertamenti sanitari di idoneità alla mansione specifica;
- relazione su sopralluogo Medico competente.

8. *Documentazione tecnica:*
   - planimetria e layout aggiornato;
   - certificato di usabilità dei locali;
   - dichiarazione di conformità impianto elettrico;
   - denuncia e verifica impianto di messa a terra;
   - documentazione generatori di calore e libretto di centrale;
   - libretti di uso e manutenzione delle macchine/attrezzature;
   - schede di sicurezza prodotti chimici utilizzati.

4.4 Flussi verso l'Organismo di Vigilanza

Sono da prevedere flussi all'OdV nei seguenti casi:

- Segnalazioni, ripetizioni ed aggiornamenti:
  - documenti di valutazione del rischio;
  - adempimenti formali di nomina delle cariche assegnate ai vari responsabili (RSPP, MC) e addetti a compiti speciali;
  - certificato di prevenzione incendi e registro antincendi con i vari aggiornamenti;
  - documentazione tecnico-procedurale.
- Segnalazioni ad evento:
  - tutti i casi di infortunio sul lavoro (anche quelli di minore entità);
  - risultati delle verifiche sulla sicurezza dei luoghi di lavoro e delle attrezzature effettuate da qualunque ente esterno;
  - risultati delle verifiche sulla sicurezza dei luoghi di lavoro effettuate da enti interni.

5. PROCEDURE SPECIFICHE

Per una corretta attuazione di quanto stabilito nel precedente § 1, **la Società assicura** la emissione, la effettiva e coerente applicazione e l'adeguamento nel tempo delle seguenti specifiche procedure/disposizioni:

a. definizione formale delle funzioni di responsabilità in materia di sicurezza;
b. organizzazione degli accertamenti sanitari preventivi e periodici e gestione dei relativi risultati;
c. gestione di pronto soccorso, emergenza, evacuazione e prevenzione incendi;
d. gestione amministrativa delle pratiche di infortunio e delle malattie professionali.

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "D"

Aree di attività nel cui ambito possono essere commessi i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita (art. 25 *octies* del D. Lgs. 231/2001)

B.E.E. Team spa *–Tutti i diritti riservati.*

1. PREMESSA

La Parte Speciale D riguarda i reati commessi in violazione delle norme sulla prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo, riferendosi a comportamenti relativi alle corrispondenti fattispecie indicate .

Obiettivo della presente disciplina è che tutti i soggetti interessati tengano comportamenti conformi a quanto prescritto nel Modello al fine di prevenire la commissione dei reati inseriti nel corpus del D. Lgs. 231/01, all'art. 25 octies, con la c.d. III Direttiva Antiriciclaggio (Decreto Legislativo n. 231 del 21 novembre 2007).

2. PROCESSI SENSIBILI

I principali processi sensibili alla commissione dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita possono essere così riassunti:

Rapporti con soggetti terzi

1. Acquisti di beni e servizi
2. Vendite
3. Finanza dispositiva

Rapporti *infragruppo*

1. Acquisti di beni e servizi
2. Vendite
3. Finanza dispositiva

A titolo esemplificativo delle concrete modalità di commissione dei reati in argomento, in riferimento ai processi sopra richiamati si possono menzionare:

- Acquisti/Ciclo Passivo; ricezione di beni derivanti in realtà dalla commissione di delitti (quali, ad esempio, programmi informatici contraffatti) da parte di fornitori dei quali non sia stata adeguatamente verificata la correttezza e professionalità della Società deputata alla selezione;
- Acquisti/Rapporti intercompany pagamento di una prestazione erogata in favore della Società da altra società facente parte del Gruppo realizzato attraverso l'impiego di somme provenienti dalla commissione di delitti (ad esempio, false comunicazioni sociali).
- Finanza dispositiva/Gestione dei pagamenti flusso finanziario per il saldo di una fattura relativa ad una prestazione erogata da terzi proveniente da precedenti transazioni saldate tramite l'apporto di denaro proveniente da delitti commessi da una controparte contrattuale.

B.E.E. Team spa *–Tutti i diritti riservati.*

- Finanza dispositiva/Partecipazioni pagamento di un corrispettivo per una partecipazione di minoranza in una entità legale italiana od estera realizzato per un importo esuberante il valore della partecipazione acquisita.
- Vendite/Ciclo attivo flusso finanziario per il saldo di una fattura relativa ad una prestazione erogata dalla Società proveniente da delitti commessi dalla controparte contrattuale.

I processi sopra individuati, esposti al rischio di commissione dei reati di riciclaggio e ricettazione di cui si tratta nella presente Parte Speciale, possono altresì dare luogo, sempre in relazione alle medesime fattispecie di reato, anche ai delitti di criminalità organizzata. Ne deriva che i protocolli di prevenzione e controllo, nel seguito indicati, costituiscono un presidio di contrasto anche in riferimento ai reati associativi, oltre agli specifici principi di carattere generale di cui alla Parte Speciale F.

3. REGOLE GENERALI

3.1 Il sistema in linea generale

Obiettivo della presente Sezione è che chiunque possa essere coinvolto nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati qui considerati, si attenga a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

In particolare, nell'espletamento di tali attività, è espressamente vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita,.

Nello svolgimento delle operazioni attinenti le Attività di Rischio, oltre alle regole previste dal Modello, i Destinatari di questo sistema di prevenzione, sono tenuti a rispettare:

8. la normativa italiana e straniera applicabile;
9. il Codice Etico;
10. il sistema di controllo interno (le procedure/linee guida aziendali, la documentazione e le disposizioni circa la struttura organizzativa e il sistema di controllo della gestione);
11. le norme inerenti il sistema amministrativo, contabile, finanziario, di *reporting* della società.

3.2 Principi generali di comportamento

E' fatto espresso divieto a coloro che, per attività o funzione svolta, si trovino ad operare nelle citate Aree di Rischio, di porre in essere, ovvero dare causa a condotte che integrino, direttamente o indirettamente, i reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienze illecita.

Conseguentemente, i soggetti come sopra identificati hanno l'espresso obbligo di:

- verificare l'attendibilità commerciale e professionale dei fornitori e dei partner commerciali/ finanziari, sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici – protesti, procedure concorsuali o acquisizione di informazioni commerciali sull'azienda, sui soci e sugli amministratori tramite società specializzate, entità del prezzo sproporzionata rispetto ai valori medi di mercato, ecc.)
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nella transazioni;
- effettuare controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte (esempio paradisi fiscali, paesi a rischio terrorismo, ecc.), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e istituti che non hanno insediamenti fisici in alcun paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie, verificare sulla tesoreria (rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretto al portatore o anonimo per la gestione della liquidità, ecc.);
- determinare i requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard;
- identificare una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard;
- identificare l'organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità;
- determinare criteri di selezione, stipulazione ed esecuzione di accordi/*joint venture* con altre imprese per la realizzazione di investimenti. Trasparenza e tracciabilità degli accordi/*joint venture* con altre imprese per la realizzazione di investimenti;
- verificare la congruità economica di eventuali investimenti effettuati in *joint venture* (rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di *due diligence*);
- adottare adeguati programmi di informazione del personale ritenuto esposto al rischio riciclaggio.

3.3 Attività dell'Organismo di Vigilanza

L'Organismo di Vigilanza deve verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà e la puntuale applicazione degli aspetti di seguito riportati a titolo esemplificativo:

- Verifica dell'attendibilità commerciale e professionale dei fornitori e dei partner commerciali/finanziari, sulla base di alcuni indici rilevanti (es. entità del prezzo, qualità del prodotto, condizioni dell'offerente, ecc.).
- Controlli formali e sostanziali dei flussi finanziari aziendali.
- Controllo dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard.
- Verifica dell'adeguatezza della funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard.
- Verifica dell'adeguatezza dell'identificazione di un organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità.
- Verifica dell'adeguatezza dei criteri di selezione, stipulazione ed esecuzione di accordi/joint-venture con altre imprese per la realizzazione di investimenti.

Inoltre, è il compito dell'Organismo di Vigilanza di:

- sovrintendere alla somministrazione di adeguati programmi di formazione ed informazione del personale ritenuto esposto al rischio riciclaggio;
- verificare periodicamente – con il supporto delle altre funzioni competenti – il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile interno od ai sub responsabili;
- comunicare tempestivamente al Consiglio di Amministrazione le eventuali infrazioni alle disposizioni – normative e procedurali – rilevanti in materia di prevenzione dei fenomeni di riciclaggio.

3.4 Flussi verso l'Organismo di Vigilanza

Devono essere segnalate all'Organismo di Vigilanza/Comitato di Controllo le operazioni effettuate in deroga ai principi sopra elencati in riferimento agli specifici processi aziendali a rischio reato ed in concomitanza con i flussi periodici previsti nella Parte Speciale A.

4. PROCEDURE SPECIFICHE

Per una corretta attuazione di quanto stabilito nel § 3, vale l'osservanza delle specifiche disposizioni inserite nelle procedure aziendali relativamente ai processi sensibili richiamati in precedenza.

PARTE SPECIALE "E"

Aree di attività nel cui ambito possono essere commessi i reati informatici previsti dall'articolo 24 bis del D. Lgs. 231/01 (introdotto dalla Legge 48/2008)

B.E.E. Team spa *–Tutti i diritti riservati.*

1. PREMESSA

Il D. Lgs. 231/01 ha recepito con la Legge n. 48, art. 7, del 18 marzo 2008, pubblicata in G.U. n. 80 del 4 aprile 2008, la Convenzione del Consiglio d'Europa sulla criminalità informatica, redatta a Budapest il 23 novembre 2001.

A seguito della ratifica ed esecuzione della Convenzione suddetta dopo l'art. 24 del D. Lgs. 231/01 è stato inserito l'art. 24bis "Delitti informatici e trattamento illecito di dati", trattati nella presente Parte Speciale E.

2. FUNZIONE DELLA PARTE SPECIALE

Il D.Lgs. 231/01 ha recepito con la Legge n. 48, art. 7, del 18 marzo 2008, pubblicata in G.U. n. 80 del 4 aprile 2008, la Convenzione del Consiglio d'Europa sulla criminalità informatica, redatta a Budapest il 23 novembre 2001.

A seguito della ratifica ed esecuzione della Convenzione suddetta dopo l'art. 24 del D.Lgs. 231/01 è stato inserito l'art. 24*bis* "Delitti informatici e trattamento illecito di dati", trattati nella presente Parte Speciale E.

Obiettivo della presente parte speciale è garantire che i soggetti Destinatari (v. nel seguito) mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati di cui si tratta.

Nella Parte Generale sono stati richiamati i principi ispiratori della normativa e i presidi principali per l'attuazione delle vigenti disposizioni in materia. In questa Parte Speciale sono individuati i principi di riferimento per la costruzione del modello di organizzazione, gestione e controllo, specificamente previsti in relazione alle fattispecie di attività sensibili individuate al fine di prevenire la commissione dei reati informatici di cui all'art. 24*bis* del D.Lgs. 231/01 e dei delitti in materia di violazione del diritto d'autore, previsti dall'art. 25 *novies* del D.Lgs. 231/01 (introdotto dalla Legge 99/2009) e di seguito descritti.

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema previsto dal decreto.

Il recepimento della convenzione ha esteso la responsabilità amministrativa degli enti ai seguenti reati informatici:

- *accesso abusivo ad un sistema informatico o telematico* (**art. 615*ter* c.p.**);
- *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (**art. 617*quater* c.p.**);
- *installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche* (**art. 617*quinquies* c.p.**);
- *danneggiamento di informazioni, dati e programmi informatici* (**art. 635*bis* c.p.**);
- *danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da latro ente pubblico o comunque di pubblica utilità* (**art. 635*ter* c.p.**);

- *danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità* (**art. 635*quater* c.p**.);
- *danneggiamento di sistemi informatici o telematici di pubblica utilità* (**art. 635*quinquies* c.p.**);

con previsione di sanzione pecuniaria da cento a cinquecento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere a), b) ed e).

- *detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici* (**art. 615*quater* c.p**.);
- *diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (**art. 615*quinqiues* c.p**.);

con previsione di sanzione pecuniaria sino a trecento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere b) ed e).

- *falsità in un documento informatico pubblico o avente efficacia probatoria* (**art. 491*bis* c.p**.);
- *frode informatica del certificatore di firma elettronica (**art. 640quinquies c.p.**).*

con previsione di sanzione pecuniaria sino a quattrocento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere c), d) ed e).

Con la Legge 23.07.2009, n. 99 è stata prevista la responsabilità amministrativa degli Enti in relazione anche ai reati in materia di protezione del diritto d'autore e di altri diritti connessi al suo esercizio. Si tratta, più in particolare, di alcune delle fattispecie di reati posti a tutela del diritto dell'autore e allo sfruttamento esclusivo delle opere dell'ingegno che sanzionano nello specifico:

- la messa a disposizione del pubblico, tramite l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette o di parti di esse, ivi comprese quelle non destinate alla pubblicazione, ovvero l'usurpazione della paternità dell'opera, la deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti un'offesa all'onore od alla reputazione dell'autore (art. 171, co. 1, letto a-*bis*) e 3);
- la duplicazione abusiva, per trarne profitto, di programmi per elaboratore ovvero l'importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o la concessione in locazione, sempre al fine di trarne profitto, di programmi contenuti in supporti non contrassegnati dalla SIAE, ovvero di mezzi di qualsiasi tipo intesi unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori (art. 171-*bis*, co. 1);
- la riproduzione, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o dimostrazione in pubblico, al fine di trarne profitto, su supporti non contrassegnati SIAE, di una banca di dati in violazione delle disposizioni di legge a tutela dei diritti dell'autore (artt. 64-*quinquies* e 64-*sexies*), ovvero l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di legge a tutela dei diritti del costitutore della banca di dati (artt. 102-*bis* e 102-*ter*), ovvero la distribuzione, vendita o concessione in locazione di una banca dati (art. 171-*bis*);

- se commesse a scopo di lucro e non a fini personali, la duplicazione abusiva, la riproduzione, la trasmissione, la diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, ovvero, anche al di fuori delle ipotesi di concorso, l'introduzione nel territorio dello Stato, la detenzione per la vendita, la distribuzione, il commercio, la concessione in noleggio o la cessione, proiezione in pubblico, trasmissione a mezzo della televisione, radio, la diffusione in pubblico di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, di dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fotogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento, di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, nonché qualsiasi supporto contenente opere dell'ingegno per le quali è richiesta l'apposizione del contrassegno SIAE, ovvero di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto (art. 171-*ter*, lett. a, b, c, d e f);
- la ritrasmissione o diffusione, in assenza di accordo con il legittimo distributore, con qualsiasi mezzo, di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato (art. 171-*ter*, lett. e);
- la fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per vendita o noleggio, la detenzione per scopi commerciali di qualsiasi mezzo o servizio idoneo ad facilitare l'elusione delle misure tecnologiche poste a protezione delle opere o dei materiali protetti ovvero la rimozione delle informazioni elettroniche sul regime dei diritti (art. 171-*ter*, lett. f-*bis* e h);
- la mancata comunicazione entro 30 giorni dalla data di immissione in commercio sul territorio nazionale dei dati necessari alla univoca identificazione dei supporti non soggetti al contrassegno, ovvero la falsa dichiarazione relativa all'avvenuto assolvimento degli obblighi in materia di contrassegno SIAE (art. 181-*bis*, co, 2) (art. 171-*septies*);
- la produzione, messa in vendita, importazione, promozione, installazione, modificazione, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, satellite, cavo, in forma sia analogica sia digitale (art. 171-*octies*).

3. DESTINATARI DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari siano consapevoli della valenza dei comportamenti tenuti e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

4. PROCESSI SENSIBILI

Le aree aziendali in cui può verificarsi il rischio che siano commessi i reati informatici previsti dall'articolo 24-bis del D. Lgs. 231/2001 sono, teoricamente, tutte quelle in cui le attività sono supportate da sistemi informatici e/o telematici per la elaborazione e trasmissione di dati (gestionali, contabili, fiscali, ecc). La prevenzione dei crimini informatici deve essere svolta attraverso adeguate **misure organizzative, tecnologiche e normative**.

Per quanto concerne le **attività sensibili** individuate, con riferimento ai reati informatici richiamati dall'art. 24-bis del D. Lgs. 231/2001, si evidenzia che qualsiasi attività aziendale che contempli la gestione, la manutenzione e l'utilizzo di sistemi informatici, database, piattaforme e strutture ICT in genere, può astrattamente ritenersi a rischio.

A titolo esemplificativo delle modalità attraverso le quali potrebbero essere realizzati i reati in esame si menzionano:

- l'accesso abusivo ad un sistema informatico o telematico facente capo ad un concorrente per acquisire informazioni a scopo di spionaggio industriale;
- l'accesso abusivo ad un sistema informatico o telematico facente capo a concorrenti, enti detentori di informazioni di interesse ovvero potenziali clienti allo scopo di implementare la propria offerta commerciale o le proprie strategie di marketing;
- l'accesso abusivo ad un sistema informatico o telematico di una banca o di una pubblica amministrazione, allo scopo di modificare i dati relativi alla Società;
- l'accesso abusivo ad un sistema informatico o telematico facente capo alla Società medesima, allo scopo, ad esempio, di manipolare i dati destinati a confluire nel bilancio;
- l'accesso abusivo ad un sistema informatico o telematico facente capo ad un cliente per modificare i dati relativi ad una commessa effettuata o in corso di effettuazione da parte della Società (ad esempio, sistemi di fatturazione od ordinativi);
- l'intercettazione fraudolenta di comunicazioni tra i dipendenti al fine di conoscere preventivamente eventuali strategia in sede sindacale o di verificarne la produttività;
- l'intercettazione fraudolenta di comunicazioni di enti concorrenti nel contesto di una partecipazione ad una gara di appalto o di fornitura svolta sul base elettronica al fine di falsarne o conoscerne preventivamente l'esito;
- l'impedimento/interruzione di una comunicazione al fine di ostacolare un concorrente nell'invio della documentazione relativa ad una gara ovvero di materiale destinato alla clientela in modo da determinarne l'inadempimento;
- il danneggiamento dei sistemi informatici/telematici facenti capo ad un concorrente al fine di impedirne l'attività o comprometterne l'immagine;

- il danneggiamento dei sistemi informatici/telematici facenti capo ad una controparte commerciale al fine di poter procedere alla fornitura di nuovi prodotti o di dimostrare l'inaffidabilità di quelli in precedenza forniti da un concorrente;
- il danneggiamento, la distruzione o la manomissione di documenti informatici aventi efficacia probatoria presenti negli archivi di pubbliche amministrazioni nell'interesse della Società;
- la messa a disposizione, immettendola in un sistema di reti telematiche di file audio, video, programmi per elaboratore, disegni industriali tutelati da diritto d'autore al fine di agevolare l'operatività di specifiche funzioni aziendali;
- la duplicazione abusiva di un programma informatico per la successiva distribuzione ad altre Società del Gruppo o a terzi affinché possano utilizzarlo nella loro operatività corrente;
- l'utilizzo abusivo di opere dell'ingegno (ad esempio, disegni industriali) illegittimamente acquisiti presso un concorrente per rendere più efficiente la produzione.

La macroaree di attività a rischio sono le seguenti:

- sistemi informativi di gestione aziendale,
- servizi applicativi finanziario/gestionali,
- elaborazione delle informazioni di carattere finanziario/gestionale,
- attività di gestione, e/o amministrazione, e/o manutenzione dei sistemi IT,
- sistemi informativi di supporto alla produzione.

Particolare attenzione è rivolta alle **attività di gestione e monitoraggio** degli accessi ai sistemi IT, nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione,
- gestione e protezione della postazione di lavoro,
- gestione degli accessi verso l'esterno,
- gestione e protezione delle reti,
- gestione degli output di sistema e dei dispositivi di memorizzazione,
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.).

Oltre ai presidi di carattere generale che disciplinano gli aspetti etico -comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, B.E.E TEAM ha provveduto ad identificare i seguenti specifici presidi organizzativo/gestionali:

- gestione delle architetture di firewalling atte a separare gli ambienti in modo da identificare le minacce a seconda della rete di provenienza (internet o intranet) e, all'interno del perimetro di rete intranet, a separare gli ambienti di produzione da quelli office gestione delle profilazioni utente in base alle funzioni preposte e alle relative competenze, in modo da garantire l'operatività su dati e applicazioni sulla base di ruoli e responsabilità;
- gestione di sistemi IDS per il monitoraggio e la registrazione di tutti i tentativi di accesso non autorizzato, con la relativa analisi da parte dei responsabili della sicurezza infrastrutturale;

Allo stesso modo è utile richiamare il rispetto di leggi e regolamenti relativi alla *protezione e sicurezza di dati personali e sistemi informatici*: ***Codice in materia di protezione dei dati personali*** (D. Lgs. 196/2003), ***provvedimenti del Garante Privacy***, regolamenti e procedure sugli abusi di mercato, ecc. Ad esempio, nell'ambito delle previsioni del codice privacy, assumono rilevanza le misure di protezione fisica dei sistemi, dei dati e dei programmi informatici, fra le quali:

- installazione e gestione di sistemi di allarme, antifurto, antincendio, eccetera;
- installazione e gestione di apparecchiature di continuità dell'energia elettrica;
- installazione, gestione ed aggiornamento di programmi antivirus;
- controllo degli accessi ai locali del centro elaborazione dati;
- inventario periodico delle attrezzature hardware, dei programmi e delle licenze d'uso;
- assegnazione di codici di accesso personalizzati in funzione dei ruoli e dei compiti attribuiti al personale che utilizza i sistemi informatici/telematici;
- conservazione dei codici di accesso in luoghi protetti e gestione delle sostituzioni;
- sistemi di periodico dei dati;
- sistemi di conservazione dei programmi applicativi e dei supporti di back-up.

Secondo gli approcci sopra descritti, gli obiettivi fondamentali della sicurezza informatica che B.E.E TEAM si pone sono i seguenti:

- ***Riservatezza****:* garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- ***Integrità****:* garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- ***Disponibilità****:* garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

I processi sopra individuati, esposti al rischio di commissione dei reati in materia informatica e di diritto d'autore di cui si tratta nella presente Parte Speciale, possono altresì dare luogo, sempre in relazione alle medesime fattispecie di reato, anche ai delitti di criminalità organizzata. Ne deriva che i protocolli di prevenzione e controllo, nel seguito indicati, costituiscono un presidio di contrasto anche in riferimento ai reati associativi, oltre agli specifici principi di carattere generale di cui alla Parte Speciale F.

5. REGOLE GENERALI

5.1 Il sistema in linea generale

Obiettivo della presente Sezione è che chiunque possa essere coinvolto nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati qui considerati, si attenga a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire comportamenti che integrino, direttamente o indirettamente, i delitti informatici o il trattamento illecito dei dati.

Ciò posto, con specifico riguardo alle problematiche connesse al rischio informatico, B.E.E TEAM, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci **politiche di sicurezza informatica**. In particolare, tale sicurezza viene perseguita attraverso la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e la garanzia della massima continuità del servizio.

Sulla base degli standard di riferimento internazionali, per **sistema aziendale di sicurezza informatica** si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

5.2 Principi generali di comportamento

Sulla base dei principi generali declinati in precedenza, la presente parte speciale prevede l'espresso divieto a carico dei Destinatari, come sopra definiti, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle richiamate nella presente parte speciale (art. 24-bis del D. Lgs. 231/2001);
- porre in essere, collaborare o dare atto alla realizzazione di comportamenti i quali, sebbene non risultino tali da costituire reato, possano potenzialmente diventarlo;
- violare i principi e le procedure aziendali previste nella presente parte speciale, oltre alle altre norme aziendali o di Gruppo contenute, ad esempio, nel "Codice Etico", nelle "Regole aziendali per l'utilizzo dei sistemi informatici e le forme di controllo dei lavoratori", nel "Documento Programmatico sulla Sicurezza", ecc.
- Nell'ambito delle suddette regole, è **fatto divieto**, in particolare, di:

  a. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
  b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
  c. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;

d. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
e. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
f. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
g. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
h. istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
i. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
j. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
k. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
- in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
- evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dal responsabile dei Sistemi Informativi o la cui provenienza sia dubbia;
- evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa o di altra società del

Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;

- evitare di diffondere, comunicare o lasciare incustodite le proprie password di accesso, codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico o telematico della Società;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, ecc);
- evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi (Custode delle credenziali), che provvederà immediatamente alla sua sostituzione;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
- evitare di installare/utilizzare in modo non appropriato apparecchiature hardware, anche esterne rispetto a personal computer e pc portatili che possano contenere programmi o software potenzialmente dannosi per il sistema;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

E' altresì fatto obbligo:

a. agli Amministratori di Sistema di denunciare al Responsabile della funzione amministrativa eventuali accessi al sistema informatico aziendale da parte di hacker;

- ai dipendenti, dirigenti ed amministratori di attenersi al Regole aziendali per l'utilizzo dei sistemi informatici e le forme di controllo dei lavoratori" "Regole aziendali

per l'utilizzo dei sistemi informatici e le forme di controllo dei lavoratori" e DPSS[4] relativo a: utilizzo del personal computer;

- utilizzo della rete;
- gestione delle password;
- utilizzo dei supporti magnetici;
- utilizzo dei pc portatili;
- uso della posta elettronica;
- policy in materia di privacy e riservatezza del know-how.

E', comunque, necessario:

- che sia garantito il rispetto del Codice Etico;
- che tutte le attività e le operazioni svolte per conto di B.E.E TEAM siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza.

5.3 Principi del sistema di controllo per la prevenzione dei reati informatici e delle violazioni del diritto d'autore.

Il sistema di controllo per la prevenzione dei reati di criminalità informatica dovrà basarsi, ove applicabili, sui seguenti **principi di controllo**:

- **Segregazione delle attività** *[Separazione dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio]* - Si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di (i) gestione di un processo e di controllo dello stesso, (ii) progettazione ed esercizio, (iii) acquisto di beni e risorse e relativa contabilizzazione.
- **Esistenza di procedure/norme/circolari**: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma**: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società.
- **Tracciabilità degli accessi e delle attività svolte sui sistemi informatic**i che supportano i processi esposti a rischio. Ogni operazione relativa all'attività sensibile deve

4 - Documento Programmatico sulla Sicurezza con i contenuti minimi indicati alla regola 19 dell'allegato B del D.Lgs. 196/03 deve essere obbligatoriamente tenuto dall'"Amministratore di sistema".

essere adeguatamente tracciata/registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità.

Inoltre si richiede:

- chiara definizione delle responsabilità delle funzioni preposte alle attività di gestione dei sistemi informativi;
- procedure e livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio;
- raccolta, analisi e gestione di segnalazioni di fattispecie a rischio di reati informatici rilevati da soggetti interni e esterni all'ente;
- procedure di *escalation* per la gestione di fattispecie a rischio di reato caratterizzate da elevata criticità e la gestione dei rapporti con gli Enti Istituzionali.

6. ATTIVITÀ DELL'ORGANISMO DI VIGILANZA

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili. Di detti controlli l'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale, secondo le modalità previste nella Parte Generale del presente Modello.

7. FLUSSI VERSO L'ORGANISMO DI VIGILANZA

E' compito dei Responsabili di Funzione informare l'Organismo di Vigilanza circa:

- la piena conoscenza da parte dei vari Responsabili e dei sottoposti del processo da seguire e degli obblighi da osservare nello svolgimento dell'operazione, con dichiarazione di conformità al D. Lgs. 231/01;

- l'elencazione dei principali adempimenti effettuati nell'espletamento dell'attività di controllo e verifica;
- anomalie e deroghe eventuali alle procedure di accesso ai sistemi informatici/telematici.

8. PROCEDURE SPECIFICHE

Ai fini dell'attuazione delle regole elencate nei precedenti capitoli, oltre che dei principi generali contenuti nella parte generale del modello e dei principi generali di controllo, nel disciplinare la fattispecie di attività sensibile di seguito descritta, deve essere predisposta ed applicata una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:

- definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
- costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
- puntuale pianificazione delle attività di sicurezza informatica;
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la business continuity attraverso meccanismi di superamento di situazioni anomale;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "F"

Reati di criminalità organizzata previsti dall'articolo 24 *ter* del D.Lgs. 231/01 (introdotto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29) e reati transnazionali (di cui all'art. 10 della Legge 26/03/2006, n. 146)

B.E.E. Team spa *–Tutti i diritti riservati.*

1. PREMESSA

L'art. 2, co. 29, della Legge 15 luglio 2009 n. 94 ha introdotto all'art. 24 *ter* del D.Lgs. 231/01 la responsabilità amministrativa degli enti in relazione ai reati di criminalità organizzata (c.d. "delitti associativi").

In precedenza, l'art. 10 della Legge 26/03/2006, n. 146 aveva introdotto la responsabilità amministrativa degli enti in relazione ad una serie di reati commessi con modalità transnazionale, vale a dire quelli nei quali sia coinvolto un gruppo criminale organizzato e che:

a) siano commessi in più di uno Stato;
b) ovvero siano commessi in uno Stato, ma una parte sostanziale della loro preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
c) ovvero siano commessi in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
d) ovvero siano commessi in uno Stato ma abbiano effetti sostanziali in un altro Stato.

I reati associativi, ed in particolare quelli di cui agli artt. 416 e 416-bis c.p., si caratterizzano per la natura stabile e permanente dell'accordo criminoso tra i soggetti che costituiscono, partecipano, promuovono od organizzano l'associazione.

A tal fine, l'associazione necessita di una seppur minima organizzazione a carattere stabile, adeguata a realizzare gli obiettivi criminosi e destinata a durare anche oltre la realizzazione – peraltro meramente eventuale – dei delitti concretamente programmati. L'associazione – che deve essere formata almeno da tre persone – si contraddistingue altresì per l'indeterminatezza del programma criminoso perseguito dagli associati che non devono dunque avere di mira la realizzazione di un numero determinato e definito di illeciti.

In virtù dell'estensione operata dall'art. 10 Legge 146/2006, il reato associativo è presupposto della responsabilità dell'ente anche nell'ipotesi in cui sia commesso con modalità transnazionale.

La responsabilità dell'ente è prevista anzitutto in relazione alla generica figura dell'associazione per delinquere, che si caratterizza per il mero scopo degli associati di commettere più delitti: al riguardo, è opportuno evidenziare che tra i reati scopo dell'associazione, può rientrare qualsiasi delitto, quali, ad esempio, la truffa, i delitti tributari, i delitti ambientali, il riciclaggio, la corruzione, i delitti societari, ecc.

La punibilità dell'ente è oggi peraltro espressamente estesa anche alle associazioni che perseguano lo specifico scopo di realizzare il traffico illecito di sostanze stupefacenti o psicotrope, nonché dell'illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o di tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, ovvero, nella forma transnazionale, del contrabbando di tabacchi lavorati esteri e del traffico di migranti.

In ragione della peculiare struttura dei reati in esame, è opportuno evidenziare che - al fine di evitare indebite estensioni dell'ambito applicativo del Decreto ed in ossequio al principio di legalità sancito

B.E.E. Team spa *–Tutti i diritti riservati.*

all'art. 2 - i criteri dell'interesse o del vantaggio dovranno essere riferiti al delitto associativo e non già ai delitti-scopo del sodalizio criminoso.

Inoltre, come già evidenziato, ai fini della sussistenza dell'illecito, non è necessario che detti illeciti siano effettivamente commessi, essendo sufficiente che siano semplicemente ricompresi tra gli scopi dell'associazione.

La punibilità dell'ente è prevista anche per il reato di associazione di tipo mafioso che, ai sensi dell'art. 416-bis, co. 3, sussiste quando coloro che ne fanno parte si avvalgono del c.d. metodo mafioso, che si concretizza nella 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, concessioni, autorizzazioni, appalti o servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

È opportuno al riguardo evidenziare che la punibilità dell'ente può conseguire, oltre che dalla partecipazione di suoi soggetti apicali o dipendenti all'associazione, in qualità di organizzatori, promotori, membri o dirigenti della stessa, anche in relazione all'ipotesi di c.d. concorso esterno, ossia quando la persona fisica, pur non facendo effettivamente parte dell'associazione e non avendo aderito agli scopi indeterminati ed illeciti che essa persegue, fornisca supporto all'organizzazione anche rispetto a specifiche attività o interessi della medesima.

È altresì importante distinguere, ai fini della corretta individuazione dei profili di rischio connessi ai reati in esame, che solo in ipotesi estreme e affatto peculiari l'ente può essere considerato esso stesso una vera e propria associazione finalizzata alla commissione di una pluralità di delitti, ipotesi cui consegue, a norma dell'art. 14, co. 4, l'interdizione definitiva dall'attività. Al riguardo, la Relazione al Decreto e l'art. 10, co. 4, della Legge 146/2006 forniscono importanti elementi interpretativi: tale identificazione, infatti, è possibile soltanto nell'ipotesi in cui "l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati".

Per tale ragione, si ritiene che, al di là di tale ipotesi estrema, i maggiori profili di rischio connessi all'operatività societaria insistono nello svolgimento di attività che comportino contatti con soggetti esterni che facciano parte di associazioni a delinquere già esistenti cui gli esponenti aziendali potrebbero fornire consapevole supporto, in vista del perseguimento anche di presunti interessi sociali.

La responsabilità dell'ente è infine prevista per il reato di sequestro di persona a scopo di rapina ed estorsione (art. 630 c.p.), fattispecie che si configura nel caso di sequestro di una persona allo scopo di perseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione. Il reato è aggravato nel caso in cui dal sequestro derivi la morte non voluta della persona sequestrata.

Si tratta di un'ipotesi di minore rilevanza quanto al contesto societario, ancorché non possano escludersi casi di concorso dell'esponente aziendale con associazioni criminali che, allo scopo di ottenere illeciti vantaggi, sequestrino, ad esempio in Paesi esteri, dipendenti della Società o del Gruppo al fini di ottenere un riscatto o altri vantaggi (l'ottenimento di un appalto). Benché tale condotta possa considerarsi, in termini generali ed astratti, scriminata dallo stato di necessità, non può escludersi che,

ricorrendo particolari condizioni (ossia la possibilità di evitare altrimenti il pericolo di vita), l'ente possa essere chiamato a rispondere in relazione all'eventuale concorso del dipendente.

2. FUNZIONE DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Destinatari del Modello Organizzativo, come meglio definiti nella Parte Generale, coinvolti in attività nelle quali sia ipotizzabile la commissione, a livello nazionale e/o transnazionale, di uno dei reati di criminalità organizzata, più precisamente:

- reati di criminalità organizzata di cui all'art. 24 *ter* del D.Lgs. 231/01 (introdotto dall'art. 2, co. 29, della Legge 15 luglio 2009 n. 94):
  - associazione per delinquere (Art. 416, co 1÷6 c.p.);
  - associazione di tipo mafioso (art. 416-*bis* c.p.);
  - sequestro di persona a scopo di estorsione (art. 630 c.p.);
  - associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, d.p.r. 09/10/1990, n. 309);
  - illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o di tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'art. 2, co. 3, Legge 18/04/1975, n. 110.

- reati commessi con modalità transnazionale (per i quali l'art. 10 della Legge 26/03/2006, n. 146 ha previsto la responsabilità amministrativa degli enti):
  - associazione per delinquere (art. 416 c.p.);
  - associazione di tipo mafioso (art. 416-*bis* c.p.);
  - associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, d.p.r. 09/10/1990, n. 309);
  - associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater*, d.p.r. 23/01/1973, n. 43);
  - traffico di migranti, per i delitti di cui all'art. 12, co. 3, 3-*bis*, 3-*ter* e 5, del testo unico di cui al D.Lgs. 25/07/1998, n. 286.

Obiettivo della presente Parte Speciale è garantire che i soggetti di cui sopra si comportino in conformità ai principi di riferimento in essa riportati medesima, al fine di prevenire la commissione dei reati di cui si tratta.

3. DESTINATARI DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari siano consapevoli della valenza dei comportamenti tenuti e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

4. PROCESSI SENSIBILI

In relazione alla commissione dei delitti di criminalità organizzata, i processi aziendali per i quali si è valutata una maggiore esposizione al rischio sono:

- Finanza agevolata
- Acquisti di beni e servizi
- Selezione del personale
- Finanza dispositiva e tesoreria
- Consulenze e prestazioni professionali
- Gestione contenzioso e precontenzioso
- Contabilità e bilancio

Particolare attenzione dovrà essere posta alle partnership strategiche, commerciali e di approvvigionamento.

5. REGOLE GENERALI

5.1 Il sistema in linea generale

Obiettivo della presente Sezione è che chiunque possa essere coinvolto nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati qui considerati si attenga a regole di condotta conformi a quanto prescritto dalla stessa, al fine di prevenire comportamenti che integrino, direttamente o indirettamente, il reato di criminalità organizzata, sia a livello nazionale che transnazionale.

Nello svolgimento delle operazioni attinenti le attività a rischio reato, oltre alle regole previste dal Modello, i Destinatari di questo sistema di prevenzione, sono tenuti a rispettare:

- la Legge italiana e/o straniera applicabile;
- il Codice Etico;
- il sistema di controllo interno (le procedure/linee guida aziendali, la documentazione e le disposizioni circa la struttura organizzativa e il sistema di controllo di gestione).

B.E.E. Team spa *–Tutti i diritti riservati.*

5.2 Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari, come meglio definiti nella Parte Generale, di porre in essere, collaborare o dare causa alla realizzazione, a livello nazionale o transnazionale, di comportamenti:

- tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle richiamate nella presente Parte Speciale (art. 24-*bis* del D.Lgs. 231/2001 e art. 10 della Legge 26/03/2006, n. 146);
- i quali, sebbene non risultino tali da costituire di per sé fattispecie di reato, possano potenzialmente diventarlo;
- non conformi alle procedure aziendali o, comunque, non in linea con le prescrizioni espresse dal presente Modello ed i principi di cui al Codice Etico.

Tutti coloro che operano per conto della Società sono tenuti ad agire in conformità ai principi di integrità, prudenza, correttezza, trasparenza, onestà, osservando le seguenti prescrizioni:

- chiunque, agendo in nome o per conto di B.E.E. TEAM S.p.A., entri in contatto con soggetti terzi con i quali B.E.E. TEAM S.p.A. intenda intraprendere relazioni commerciali o sia con gli stessi tenuto ad avere rapporti di natura istituzionale, sociale, politica o di qualsivoglia natura, ha l'obbligo di:
  - informare tali soggetti degli impegni e degli obblighi imposti dal Codice Etico;
  - adottare le iniziative di natura interna necessarie in caso di rifiuto da parte dei soggetti terzi di adeguarsi al Codice Etico o di osservare le disposizioni contenute nel Codice stesso;
- tutti i rapporti con agenti, mediatori, intermediari e partner commerciali devono essere improntati ai principi della trasparenza e dell'integrità e devono prevedere prestazioni e compensi in linea con le prassi di mercato ed accertando che non vi siano aspetti che possano favorire la commissione di reati in Italia o all'estero, da parte di terze parti;
- verifica costante e continuativa della correttezza, effettività, congruità e rispondenza agli interessi sociali delle prestazioni richieste, erogate da parte o a favore di terzi, in modo da garantire l'instaurazione ed il mantenimento soltanto di rapporti commerciali, finanziari e consulenziali corretti, realmente rispondenti agli interessi sociali e connotati da effettività, trasparenza e congruità;
- prudenza, accuratezza ed obiettività nella selezione, individuazione o comunque nell'assunzione e prosecuzione di rapporti con soggetti terzi e nella determinazione delle condizioni afferenti al rapporto medesimo, al fine di prevenire il rischio di instaurare contatti con soggetti appartenenti ad associazioni criminose di qualsiasi natura, nazionali o transnazionali;

- rifiuto di ogni corrispettivo, in forma di denaro o altra utilità, da parte di chiunque, per l'esecuzione di un atto relativo al proprio ufficio o contrario ai doveri d'ufficio;
- rispetto della legge, dei regolamenti emessi dalle Autorità competenti e/o delle procedure interne relative alla gestione delle deleghe dei poteri di spesa;
- assoluta correttezza, trasparenza ed accuratezza nelle appostazioni contabili e negli adempimenti fiscali e nelle verifiche che ne sono presupposto.

5.3 Principi del sistema di controllo per la prevenzione dei reati

Nell'ambito dei principi generali sopra individuati, è fatto divieto in particolare di:

- instaurare rapporti con soggetti, enti, società o associazioni in qualsiasi forma costituite, in Italia o all'estero, che si sappia o si abbia ragione o sospetto di ritenere facciano parte o siano comunque legati o intrattengano rapporti di qualsiasi natura con associazioni o gruppi criminosi, ovvero comunque dei quali non si sia accertata con accuratezza, diligenza ed in modo tracciabile e documentato l'identità e la correttezza, nonché, in caso di società, l'effettiva proprietà o i legami di controllo;
- instaurare rapporti con soggetti che si rifiutino o mostrino reticenza nel fornire informazioni rilevanti ai fini della loro corretta, effettiva e completa conoscenza o rispetto ai quali sussistano elementi di sospetto in ragione anche della eventuale operatività in paesi non collaborativi, ovvero che facciano richiesta od offrano prestazioni che, pur astrattamente vantaggiose per la Società, presentino profili di sospettosità o di irregolarità, o che possano porre in essere comportamenti in contrasto con leggi e regolamenti in materia di circolazione dei capitali e dei beni, fiscale o contabile;
- introdurre in azienda armi o sostanze dannose e pericolose per la salute e sicurezza, tra cui sostanze stupefacenti.

Il sistema di controllo interno sin qui descritto, inoltre, è attuato dai protocolli di prevenzione fissati dal presente M.O. – relativamente ai processi sensibili più sopra indicati (Par. 3) - in riferimento alle altre fattispecie di reato previste dal D.Lgs. 231/01; quanto precede, fermi restando i principi generali del sistema di controllo interno di cui all'appendice B.

Ne discende che, in riferimento ai processi di:

- Acquisti di beni e servizi
- Selezione del personale
- Finanza dispositiva e tesoreria
- Consulenze e prestazioni professionali
- Gestione contenzioso e precontenzioso
- Contabilità e bilancio

B.E.E. Team spa *–Tutti i diritti riservati.*

costituiscono una efficace misura preventiva anche ai fini dei reati di criminalità organizzata, oltre che per i reati cui sono specificamente dedicati, i protocolli di prevenzione declinati, in particolare, nell'ambito delle parti speciali:

- "A" - Reati in danno della pubblica amministrazione ex art. 24 e 25 del D.Lgs. 231/01
- "B" - Reati societari ex artt. 25 *ter* e *sexies* del D.Lgs. 231/2001
- "D" - Reati di ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita ex art. 25 *octies* d.lgs. 231/01
- "E" - Reati informatici previsti dall'articolo 24 bis del D.Lgs. 231/01 (introdotto dalla legge 48/2008) e delitti in materia di violazione del diritto d'autore previsti dall'art. 25 novies (introdotto dalla legge 23.07.2009, n. 99),
- "G" – Reati di abbandono sul suolo e nel suolo di rifiuti ed acque reflue.

alla cui lettura si rinvia per i relativi dettagli ed approfondimenti.

5.4 Attività dell'Organismo di Vigilanza

È compito dell'O.d.V.:

-verificare periodicamente, con il supporto delle altre funzioni competenti, la validità di opportune clausole standard finalizzate:

- all'osservanza da parte dei collaboratori esterni e dei partner dei contenuti del Modello e del Codice Etico;
- alla possibilità di B.E.E. TEAM S.p.A. di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
- all'attuazione di meccanismi sanzionatori (quali il recesso dal contratto nei riguardi di Partner o di Collaboratori esterni) qualora si accertino violazioni delle prescrizioni;

- verificare l'osservanza, attuazione ed adeguatezza del Modello ai fini della prevenzione dei reati associativi;

-curare, in collaborazione con le funzioni aziendali di volta in volta competenti, l'emanazione e l'aggiornamento di istruzioni standardizzate relative alla compilazione omogenea e coerente, da parte dei responsabili interni:

- dei modelli di segnalazione periodica all'Organismo di Vigilanza degli eventi a rischio reato
- delle schede di evidenza del tracciamento delle attività a contatto con la P.A. (v. allegato 1).

Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

-verificare il rispetto dei protocolli procedurali, con particolare riferimento alla gestione del personale, dei rapporti con i soggetti esterni alla Società, nonché agli adempimenti contabili e tributari;

-valutare informazioni rilevanti trasmesse dalla Società.

5.5 Flussi verso il Organismo di Vigilanza

Ogni fatto od elemento dal quale si possa desumere il rischio di interferenze/infiltrazioni criminali nelle attività aziendali, in riferimento ai reati di criminalità organizzata, deve essere segnalato senza indugio dai Destinatari del M.O. all'Organismo di Vigilanza.

Quale misura sistematica di prevenzione dei reati di criminalità organizzata, devono altresì essere inviati dai responsabili interni all'Organismo di Vigilanza, nei tempi e con le modalità previste dal presente M.O. e dal quadro procedurale aziendale, i flussi di segnalazione e le schede di evidenza inerenti ai processi di loro competenza, rientranti nell'ambito di rischio più sopra individuato (Paragrafo 3 – "Processi sensibili").

6. PROCEDURE SPECIFICHE

Per una corretta attuazione di quanto stabilito nel precedente Paragrafo 4 - "Regole generali", vale l'osservanza delle specifiche disposizioni inserite nelle procedure aziendali relativamente ai processi sensibili richiamati in precedenza.

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "G"

Reati di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo (introdotti con D.Lgs. 152/2006)

B.E.E. Team spa *–Tutti i diritti riservati.*

1. PREMESSA

Con il **D.Lgs. 152/2006, all'art. 192 comma 4**, il legislatore ha voluto estendere, attraverso l'introduzione dell'articolo 25-decies (Reati ambientali), la responsabilità amministrativa dell'ente di cui al D.Lgs. 231/2001 a diverse fattispecie di "reati ambientali", come già richiesto dalla Direttiva 2008/99/CE[5] e dalla Direttiva 2009/123/CE[6], ed ha stabilito la responsabilità dell'ente in caso di commissione del reato di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo. Con riferimento a tale reato, la norma dispone che chiunque violi il relativo divieto è tenuto a procedere alla rimozione o smaltimento dei rifiuti e, nel caso in cui la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica, sono tenuti in solido la persona giuridica ed i soggetti che siano subentrati nei diritti della persona stessa, secondo le previsioni del decreto legislativo 231/2001.

Art. 192

Prescrizioni di carattere generale:

- *l'abbandono ed il deposito incontrollati di rifiuti sul suolo e nel suolo sono vietati;*
- *divieto di immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee;*
- *fatta salva l'applicazione delle sanzioni di cui agli articoli 255 e 256, chiunque viola i divieti di cui ai commi precedenti è tenuto a procedere alla rimozione, all'avvio a recupero o allo smaltimento dei rifiuti ed al ripristino dello stato dei luoghi in solido con il proprietario e con i titolari di diritti reali o personali di godimento sull'area, ai quali tale violazione sia imputabile a titolo di dolo o colpa, in base agli accertamenti effettuati, in contraddittorio con i soggetti interessati, dai soggetti preposti al controllo. Il Sindaco dispone con ordinanza le operazioni a tal fine necessarie ed il termine entro cui provvedere, decorso il quale procede all'esecuzione in danno dei soggetti obbligati al recupero delle somme anticipate;*
- *qualora la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica ai sensi e per gli effetti del comma 3, sono tenuti in solido la persona giuridica ed i soggetti che siano subentrati nei diritti della persona stessa, secondo le previsioni del decreto legislativo 8 giugno 2001 n. 231, in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni.*

Art. 255 (abbandono di rifiuti)

Prescrizioni in merito all'abbandono dei rifiuti:

[5] La Direttiva 2008/99/CE obbliga gli Stati membri a prevedere nella propria legislazione nazionale sanzioni penali in relazione a gravi violazioni delle disposizioni del diritto comunitario in materia di tutela dell'ambiente. In particolare, gli Stati membri devono provvedere affinché le persone giuridiche possano essere dichiarate responsabili dei reati ambientali richiamati dalla stessa Direttiva quando siano stati commessi a loro vantaggio.

[6] Per ulteriori informazioni sulla Direttiva, si rimanda al Portale della Normativa Sanitaria del Ministero della Salute (www.normativasanitaria.it).

- *fatto salvo quanto disposto dall'articolo 256, comma 2, chiunque, in violazione delle disposizioni di cui agli articoli 192, commi 1 e 2, 226, comma 2, e 231, commi 1 e 2, abbandona o deposita rifiuti ovvero li mette nelle acque superficiali o sotterranee è punito con la sanzione amministrativa pecuniaria da centocinque euro a seicentoventi euro. Se l'abbandono di rifiuti sul suolo riguarda rifiuti non pericolosi e non ingombranti si applica la sanzione amministrativa pecuniaria da venticinque euro a centocinquanta euro;*
- *il titolare del centro di raccolta, il concessionario o il titolare della succursale della casa costruttrice che viola le disposizioni di cui all'articolo 231, comma 5, è punito con la sanzione amministrativa pecuniaria da euro duecentosessanta a euro millecinquecentocinquanta;*
- *chiunque non ottempera all'ordinanza del Sindaco, di cui all'articolo 192, comma 3, o non adempie all'obbligo di cui all'articolo 187, comma 3, è punito con la pena dell'arresto fino ad un anno. Nella sentenza di condanna o nella sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, il beneficio della sospensione condizionale della pena può essere subordinato alla esecuzione di quanto disposto nella ordinanza di cui all'articolo 192, comma 3, ovvero all'adempimento dell'obbligo di cui all'articolo 187, comma 3.*

Art. 256 (attività di gestione di rifiuti non autorizzati)

Prescrizioni in merito all'attività di gestione di rifiuti non autorizzati:

- *chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 211, 212, 214, 215, 216 è punito:*
  - *con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti non pericolosi,*
  - *b) con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti pericolosi;*
- *le pene di cui al capoverso precedente si applicano ai titolari di imprese ed ai responsabili di enti che abbandonano o depositano in modo incontrollato rifiuti ovvero li immettono nelle acque superficiali o sotterranee in violazione del divieto di cui all'articolo 192, commi 1 e 2;*
- *chiunque realizza o gestisce una discarica non autorizzata è punito con la pena dell'arresto da sei mesi e due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la pena dell'arresto da uno a tre ani e dell'ammenda da euro cinquemiladuecento a euro cinquantaduemila se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi. Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva se di proprietà dell'autore o del compartecipe al reato, fatti salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi;*
- *le pene di cui ai commi 1, 2 e 3 sono ridotte della metà delle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesi per le iscrizioni o comunicazioni;*

- *chiunque, in violazione del divieto di cui all'art. 187, effettua attività non consentite di miscelazione di rifiuti, è punito con la pena di cui al comma 1, lettera b);*
- *chiunque viola gli obblighi di cui agli articoli 231, commi 7,8 e 9, 233, commi 12 e 13, 234, comma 14, è punito con la sanzione amministrativa pecuniaria da duecentosessanta euro a millecinquecentocinquanta euro;*
- *i soggetti di cui agli articoli 233, 234, 235 e 236 che non adempiono agli obblighi di partecipazione ivi previsti sono puniti con una sanzione amministrativa pecuniaria da ottomila euro a quarantacinquemila euro, fatto comunque salvo l'obbligo di corrispondere i contributi pregressi. Sino all'adozione del decreto di cui all'articolo 234, comma 2, le sanzioni di cui al presente comma non sono applicabili ai soggetti di cui al medesimo articolo 234;*
- *le sanzioni di cui al comma 8 sono ridotte della metà in caso di adesione effettuata entro il sessantesimo giorno dalla scadenza del termine per adempiere agli obblighi di partecipazione previsti dagli articoli 233, 234, 235 e 236.*

Art. 258 (violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari)

Prescrizioni in merito all'attività di predisposizione della documentazione di gestione di rifiuti:

- ***i soggetti di cui all'art.189 comma 3, che non effettuino la comunicazione ivi prescritta ovvero la effettuino in modo incompleto o inesatto sono puniti con la sanzione amministrativa pecuniaria da duemilaseicento euro a quindicimilacinquecento euro; se la comunicazione è effettuata entro il sessantesimo giorno dalla scadenza del termine ai sensi della legge 25 gennaio 1994 n. 70 si applicala sanzione pecuniaria da ventisei euro a centosessanta euro;***
- ***chiunque omette di tenere ovvero tiene in modo incompleto il registro di carico e scarico di cui all'art.190 comma 1, è punito con la sanzione amministrativa pecuniaria da duemilaseicento euro a quindicimilacinquecento euro. Se il registro è relativo a rifiuti pericolosi si applica la sanzione amministrativa pecuniaria da quindicimilacinquecento euro a novantamila euro, nonché la sanzione amministrativa accessoria della sospensione da un mese a un anno dalla carica rivestita dal soggetto responsabile dell'infrazione e dalla carica di amministratore;***
- ***chiunque effettua il trasporto di rifiuti senza il formulario di cui all'art. 193 ovvero indica nel formulario stesso dati incompleti è punito con la sanzione amministrativa pecuniaria da milleseicento euro a novemilatrecento euro.***

2. FUNZIONE DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Destinatari del Modello Organizzativo, come meglio definiti nella Parte Generale, coinvolti in attività nelle quali sia ipotizzabile la commissione, a livello nazionale e/o transnazionale, di uno dei reati previsti dal Decreto legislativo 3 aprile 2006, n. 152 , più precisamente:

- esercizio di una delle attività di cui all'allegato VIII del Codice dell'Ambiente (ad es. attività energetiche, produzione e trasformazione dei metalli) senza autorizzazione integrata ambientale o a seguito della sospensione o revoca della stessa (art. 29-quattuordecies);
- apertura o effettuazione di nuovi scarichi di acque reflue industriali, in assenza di autorizzazione, o mantenimento di detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata (art. 137);
- gestione di rifiuti non autorizzata ovvero: raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione (art. 256);
- bonifica dei siti ovvero: inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni della soglia di rischio (art. 257);
- traffico illecito di rifiuti ovvero: spedizione di rifiuti speciali pericolosi (tra cui rifiuti di metalli e loro leghe, rifiuti provenienti da operazioni minerarie, etc. come indicati nella lista "verde" di cui all'allegato 2 del regolamento CEE 1° febbraio 1993, n. 259) costituente traffico illecito (art. 259 primo comma);
- attività organizzate per il traffico illecito di rifiuti ovvero: cessione, ricevimento, trasporto, esportazione, importazione o gestione abusiva, con più operazioni e attraverso l'allestimento di mezzi e attività continuative ed organizzate, di ingenti quantitativi di rifiuti al fine di conseguire un ingiusto profitto (art 260);
- omessa iscrizione al sistema di controllo della tracciabilità dei rifiuti (SISTRI) (art 260-bis);
- installazione o messa in esercizio di uno stabilimento, in assenza della prescritta autorizzazione o continuazione dell'esercizio con autorizzazione scaduta, decaduta, sospesa o revocata (art. 279).

3. DESTINATARI DELLA PARTE SPECIALE

In relazione ai reati sopra esplicitati, le aree (processi) ritenute più specificamente a rischio risultano essere le operazioni poste in essere con persone fisiche e giuridiche residenti nel territorio nazionale o all'estero che trattino un'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti di qualsiasi genere.

Le procedure implementate dalla società prevedono la preventiva verifica dell'affidabilità dei fornitori e delle parti terze con le quali la Società intrattiene rapporti di fornitura di tali servizi.

Particolare attenzione viene data alla stipula di contratti ed al puntuale ed effettivo svolgimento di prestazioni concordate in conformità delle leggi vigenti.

4. PROCESSI SENSIBILI

In relazione alla commissione dei reati di cui trattasi, i processi aziendali per i quali si è valutata una maggiore esposizione al rischio sono:

- Acquisti di beni e servizi
- Finanza dispositiva e tesoreria
- Gestione verifiche ed ispezioni. Gestione rapporti con PA
- Smaltimento rifiuti ed acque reflue

Particolare attenzione dovrà essere posta alle partnership strategiche, commerciali e di approvvigionamento.

5. REGOLE GENERALI E PROCEDURE

Il presente capitolo si riferisce a comportamenti posti in essere da esponenti aziendali, consulenti e partner commerciali e parti terze.

Obiettivo del presente capitolo è che tali soggetti si attengano, nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle c.d. aree a rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della società, a regole di condotta conformi a quanto previsto nel medesimo capitolo al fine di prevenire e impedire il verificarsi dei reati di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo.

In particolare, il presente capitolo ha la funzione di:

- fornire un elenco dei principi generali e dei principi procedurali specifici cui gli esponenti aziendali, i consulenti e i partner in relazione al tipo di rapporto in essere con la società, sono tenuti d attenersi per una corretta applicazione del Modello Organizzativo;
- fornire all'ODV e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

Il presente capitolo dispone a carico degli esponenti aziendali, dei consulenti, dei partner e parti terze, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della società nell'ambito dell'espletamento delle attività considerate a rischio, di attenersi ai seguenti principi generali di condotta:

– astenersi dal porre in essere comportamenti tali da integrare i reati di abbandono o deposito incontrollato di rifiuti sul suolo e nel suolo,

- astenersi dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne.

Nell'espletamento della propria attività gli Amministratori, i Sindaci ed il personale dipendente devono rispettare le norme di comportamento di seguito indicate.

In particolare è fatto obbligo ai dipendenti ed amministratori di attenersi alle seguente procedura:

1. Gestione dei Rifiuti;

6. FLUSSI VERSO L'ORGANISMO DI VIGILANZA

E' compito della posizione organizzativa a cui riporta il Responsabile della Funzione Servizi Generali portare annualmente a conoscenza dell'OdV l'elencazione dei principali adempimenti effettuati nell'espletamento dell'attività di controllo e verifica da effettuarsi in particolare sui registri di carico e scarico, dichiarazione annuale, documento di conferimento (formulario) rifiuto firmato e datato dal ricevente.

APPENDICE

A. OPERAZIONI PROMANATE DIRETTAMENTE E "FUORI PROCEDURA" DAI SOGGETTI APICALI

4. Ambito di riferimento

I soggetti apicali secondo il D. Lgs. 231/01 sono identificati all'art. 5 come "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 ed il controllo dello stesso".

Il D. Lgs. 231/01 non ha modificato il sistema normativo che disciplina l'amministrazione ed il governo delle società, sicché l'autonomia decisionale dei soggetti in posizioni apicali è sostanziale ed indefettibile espressione della libertà di gestione dell'impresa in forma societaria.

I soggetti in posizione apicale in via ordinaria decidono operazioni che seguono i normali criteri previsti dal Modello Organizzativo, che gli stessi conoscono e condividono. Pur tuttavia tali soggetti sono talvolta necessitati – nell'interesse della società – ad avviare operazioni che seguono un iter procedimentale diverso da quello dettagliato nel Modello Organizzativo, a causa di situazioni di eccezionalità dovute ad esigenze di straordinaria urgenza o di particolare riservatezza od anche di singola peculiarità dell'operazione.

A quest'ultima tipologia di operazione si rivolge il presente Schema di Controllo Interno.

5. Attività di controllo

Il sistema di controllo si basa sui due elementi qualificanti della tracciabilità degli atti e del flusso informativo verso l'Organismo di Vigilanza.

In particolare, gli elementi specifici di controllo sono:

- Tracciabilità dell'operazione in termini di documentazione e supporti informativi atti a consentire la "ricostruibilità" a posteriori delle motivazioni e delle situazioni contingenti in cui si è sviluppata l'operazione stessa.

  Speciale riguardo deve assumere l'esplicazione, ancorché in forma sintetica (ma non generica), delle ragioni e dei motivi che hanno determinato la scelta operativa. Non necessariamente devono essere esplicitate le ragioni della decisione, ma le caratteristiche (ad es., riservatezza ed urgenza) che hanno reso impossibile l'attuazione della decisione secondo lo schema operativo prefissato;
- Specifica informativa, da parte dello stesso soggetto apicale che ha attivato l'operazione "in deroga", verso l'Organismo di Vigilanza affinché possa attuare i dovuti riscontri con sistematicità e tempestività;

B.E.E. Team spa *–Tutti i diritti riservati.*

Si sottolinea, inoltre, che un ulteriore elemento rafforzativo del sistema deriva dalla "cattura" delle operazioni "degli apicali" anche attraverso i flussi informativi riguardanti le operazioni "in deroga", previsti dai singoli Schemi di Controllo Interno sui Processi Strumentali. Tali flussi contemplano, infatti, l'invio degli estremi delle operazioni "in deroga" (a prescindere dalle origini delle stesse) all'Organismo di Vigilanza/Comitato di Controllo a cura dei Responsabili delle Funzioni materialmente esecutrici.

B. PRINCIPI GENERALI DEL CONTROLLO INTERNO

Il Sistema di Controllo Interno è l'insieme degli "strumenti" volti a fornire ragionevole garanzia circa il raggiungimento degli obiettivi di efficienza ed efficacia operativa, affidabilità delle informazioni finanziarie e gestionali, rispetto delle leggi e dei regolamenti, nonché salvaguardia del patrimonio anche contro possibili frodi.

Il Sistema di Controllo Interno si qualifica con principi generali il cui campo di applicazione si estende con continuità attraverso i diversi livelli organizzativi (Business Unit, Funzione, - nel seguito, indicati con unità organizzativa).

1. Ambiente generale di controllo

Le responsabilità devono essere definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto

Nessuna operazione significativa (in termini quali-quantitativi) per l' unità organizzativa può essere originata/attivata senza autorizzazione

I poteri di rappresentanza devono essere conferiti secondo ambiti di esercizio e limiti di importo strettamente collegati alle mansioni assegnate ed alla struttura organizzativa

I sistemi operativi devono essere coerenti con le politiche aziendali ed il Codice Etico In particolare, le informazioni finanziarie della Società devono essere predisposte:

- nel rispetto delle leggi e dei regolamenti,
- nel rispetto dei principi contabili statuiti,
- in coerenza con le procedure amministrative definite,
- nell'ambito di un completo ed aggiornato piano dei conti.

2. Valutazione dei rischi

Gli obiettivi dell' unità organizzativa devono essere definiti e comunicati a tutti i livelli interessati, al fine di rendere gli stessi chiari e condivisi

Devono essere individuati i rischi connessi al raggiungimento degli obiettivi, prevedendone periodicamente il monitoraggio e l'aggiornamento

Gli eventi negativi che possono minacciare la continuità operativa devono essere oggetto di apposita attività di valutazione dei rischi e di adeguamento delle protezioni

3. Attività di controllo

Nessuno deve avere il pieno controllo di un intero processo/attività, ma deve essere prevista a livello procedurale un'adeguata separazione dei ruoli.

I processi operativi devono essere definiti prevedendo un adeguato supporto documentale/di sistema per consentire che siano sempre verificabili in termini di congruità, coerenza e responsabilità

Le scelte operative devono essere tracciabili in termini di caratteristiche e motivazioni e devono essere individuabili coloro che hanno autorizzato, effettuato e verificato le singole attività

Lo scambio di informazioni fra fasi/processi contigui deve prevedere meccanismi (riconciliazioni, quadrature, ecc.) per garantire l'integrità e la completezza dei dati gestiti.

4. Informazioni e Comunicazione

Deve essere previsto un sistema di indicatori per processo/attività ed un relativo flusso periodico di reporting verso il management

I Sistemi Informativi amministrativi e gestionali devono essere orientati all'integrazione ed alla standardizzazione.

I meccanismi di sicurezza devono garantire la protezione/accesso fisico÷logico ai dati e ai beni di ogni unità organizzativa.

5. Monitoraggio

Il sistema di controllo è soggetto ad attività di supervisione continua e di valutazione periodica finalizzate al costante adeguamento

C. PRINCIPI DI COMPORTAMENTO CON LA PUBBLICA AMMINISTRAZIONE

Il presente documento rappresenta le linee guida di comportamento da seguire per evitare il verificarsi situazioni favorevoli alla commissione dei reati ex D. Lgs. 231/01 231.

Le linee guida si riferiscono a comportamenti relativi all'area del "comportamenti positivi" e dei "comportamenti negativi" specificando in chiave operativa quanto espresso dai principi del Codice Etico di Gruppo.

1. Area dei "comportamenti positivi"

I responsabili delle funzioni che hanno attività di contatto con la Pubblica Amministrazione devono:

- fornire ai propri collaboratori direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici, secondo le peculiarità del proprio ambito di attività, trasferendo conoscenza della norma e consapevolezza delle situazioni a rischio reato;
- prevedere adeguati meccanismi di tracciabilità circa i flussi informativi verso la P.A.

L'incarico a soggetti esterni di operare in rappresentanza di B.E.E. TEAM Spa nei confronti della P.A. deve essere assegnato in modo formale e prevedere una specifica clausola che vincoli all'osservanza dei principi etico-comportamentali adottati dalla Società.

E' fatta raccomandazione a dipendenti e collaboratori esterni di segnalare all'Organismo di Vigilanza ogni violazione o sospetto di violazione del Modello Organizzativo. Le segnalazioni devono essere fornite esclusivamente in forma non anonima.

La Società ed l'Organismo di Vigilanza tutelano dipendenti e collaboratori esterni da ogni effetto pregiudizievole che possa derivare dalla segnalazione.

L'Organismo di Vigilanza assicura la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.

Sull'intranet aziendale è disponibile, a tali fini, la casella di posta elettronica dedicata (odv.beeteam@beeteam.it)

I responsabili di funzione devono segnalare all'Organismo di Vigilanza i comportamenti a rischio di reato ex lege 231, inerenti ai processi operativi di competenza, di cui siano venuti a conoscenza in via diretta o per il tramite di informativa ricevuta dai propri collaboratori.

In particolare, in caso di tentata concussione da parte di un pubblico funzionario nei confronti di un dipendente (o altri collaboratori) sono da adottare i seguenti comportamenti:

- non dare seguito alla richiesta,
- fornire informativa tempestiva al proprio Responsabile,
- attivare formale informativa, da parte del Responsabile, verso l'Organismo di Vigilanza.

I responsabili delle funzioni che vengano ufficialmente a conoscenza di notizie, anche provenienti da organi di polizia giudiziaria, riguardanti illeciti e/o reati con rischi di impatto aziendale, devono segnalarle all'Organismo di Vigilanza.

2. Area dei "comportamenti negativi"

Con riferimento alle tipologie di reato rilevanti ai sensi del D. Lgs. 231/01, si segnalano, se pur a titolo non esaustivo, i comportamenti a rischio da evitare.

Nei rapporti con i rappresentanti della P.A. è fatto divieto di:

promettere o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali e di servizio,

promettere o concedere "soluzioni privilegiate" (ad es. interessamento per facilitare l'assunzione di parenti/affini/amici, ecc.),

effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale,

promettere di fornire o fornire impropriamente, anche tramite terzi, l'esecuzione di opere/servizi (ad es. opere di ristrutturazione di edifici privati residenziali, ecc.),

promettere o concedere omaggi/regalie dirette o indirette non di modico valore,

fornire o promettere di fornire informazioni e/o documenti riservati,

favorire, nei processi d'acquisto, fornitori e sub-fornitori in quanto indicati dai rappresentanti stessi come condizione per lo svolgimento successivo delle attività (es., affidamento della commessa, concessione del finanziamento agevolato).

I divieti sopra rappresentati si intendono estesi anche ai rapporti indiretti con i rappresentanti della P.A. attraverso terzi fiduciari.

Inoltre, nei confronti della P.A., è fatto divieto di:

- esibire documenti/dati falsi od alterati,
- tenere una condotta ingannevole che possa indurre la P.A. in errore nella valutazione tecnico-economica dei prodotti e servizi offerti/forniti,
- omettere informazioni dovute, al fine di orientare a proprio favore le decisioni della P.A.,
- destinare contributi/sovvenzioni/finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti,
- accedere in maniera non autorizzata ai sistemi informativi della P.A., per ottenere e/o
- modificare informazioni a vantaggio dell'azienda,
- abusare della posizione di gestore/manutentore dei sistemi ICT della P.A., al fine di ottenere e/o modificare informazioni a vantaggio dell'azienda.

B.E.E. Team spa *–Tutti i diritti riservati.*

D. SOGGETTI PUBBLICI INTERFACCIABILI PER IL D. LGS. 231/01

- Amministrazioni dello stato compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative ed universitarie;
- le aziende ed amministrazioni dello stato ad ordinamento autonomo;
- le regioni, le province, i comuni, le comunità montane e loro consorzi ed associazioni;
- gli istituti autonomi case popolari,
- le camere di commercio, industria, artigianato e agricoltura;
- gli enti pubblici non economici nazionali, regionali e locali;
- le amministrazioni, le aziende e gli enti del servizio sanitario nazionale,
- i concessionari di servizi pubblici, i pubblici ufficiali e gli incaricati di un pubblico servizio;
- i membri della commissione della comunità europea, del parlamento europeo, della corte di giustizia e della corte dei conti delle comunità europee;
- i funzionari e gli agenti assunti a contratto a norma dello statuto dei funzionari delle comunità europee;
- le persone comandate dagli stati membri o da qualsiasi ente pubblico o privato presso le comunità europee che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle comunità europee;
- i membri o gli addetti a enti costituiti sulla base dei trattati che istituiscono le comunità europee;
- coloro che nell'ambito di altri stati membri dell'unione europea svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- coloro che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e dell'incaricato di pubblico servizio nell'ambito di stati esteri non appartenenti all'Unione europea od organizzazioni pubbliche internazionali.

B.E.E. Team spa *–Tutti i diritti riservati.*

SCHEDA DI EVIDENZA
Rischio Reati verso le PP.AA.

Periodo:……

Responsabile Interno:……..

Premesso che:

- B.E.E. TEAM Spa S.p.A. ha predisposto il proprio Modello di Organizzazione, Gestione e controllo ai sensi del D. Lgs. 231/01;
- tale Modello è stato approvato dal Consiglio di Amministrazione del ……..

il sottoscritto dichiara che nel periodo in esame ha trattato con le Pubbliche Amministrazioni di seguito indicate le seguenti principali iniziative/attività:

Pubblica Amministrazione	Principali iniziative/attività

La presente scheda viene conservata a disposizione dell'Organismo di Vigilanza di B.E.E. TEAM Spa S.p.A.

L'eventuale documentazione a supporto egli eventi sopra evidenziati è disponibile presso i competenti Uffici della Società.

Il sottoscritto dichiara di essere a conoscenza di quanto contenuto nel Modello di Organizzazione Gestione e Controllo di B.E.E. TEAM Spa S.p.A. e non segnala, con riferimento ai propri rapporti con le Pubbliche Amministrazioni di cui sopra – ed a quelli intrattenuti con le medesime da propri collaboratori all'uopo delegati e le cui attività sono state debitamente controllate e monitorate - alcuna anomalia o infrazione al modello stesso ed, in particolare, alcun fatto o comportamento che possa riguardare l'applicazione del D. Lgs. 231/01 il cui contenuto dichiara di conoscere e di averne edotto i propri collaboratori.

……
(firma)

Data:……/……/……

Attenzione: le informazioni ed i dati contenuti nella presente scheda hanno carattere di riservatezza e non possono essere diffusi o utilizzati dall'Organismo di Vigilanza per finalità diverse da quelle definite dal Modello Organizzativo di B.E.E. TEAM Spa S.p.A.

ALLEGATO 2

FLUSSI VERSO L'ORGANISMO DI VIGILANZA

ATTIVITA' DELL'ORGANISMO DI VIGILANZA

B.E.E. Team spa –*Tutti i diritti riservati.*

Flussi verso OdV (Notizie a carattere generale)			
Tipologia delle informazioni		Ente Responsabile	Tempistica
1	Risultanze delle attività di controllo poste in essere dalle funzioni aziendali dalle quali emergano criticità	Tutti	Ad evento
2	Anomalie o atipicità riscontrate nelle attività di controllo	Tutti	Ad evento
3	Provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali su evinca lo svolgimento di indagini, anche nei confronti di ignoti , per i reati di cui al D. Lgs. 231/2001	Tutti	Ad evento
4	Avvio di contenzioso giudiziale e/o stragiudiziale da parte di clienti e fornitori	Tutti	Ad evento
5	Comunicazione interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato ai sensi di cui al D. Lgs. 231/2001 (ad es.:provvedimenti disciplinari avviati nei confronti di dipendenti)	Tutti	Ad evento
6	Le richieste di assistenza legale inoltrate dai dirigenti e/o dai quadri in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;	Tutti	Ad evento
7	Richiesta di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa, ovvero per altri reati in qualche misura collegabili con i c.d. reati-presupposto (ad es.: reati in materia tributaria che possono essere collegati a reati come le false comunicazioni sociali)	Tutti	Ad evento
8	Relazioni/comunicazioni interne ovvero l'istituzione di Commissioni di inchiesta comunque denominate, dalle quali emergano responsabilità per le ipotesi di reato di cui al D. Lgs. 231/2001	Tutti	Ad evento

B.E.E. Team spa *–Tutti i diritti riservati.*

9	Notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza - nell'ambito dei procedimenti disciplinari svolti - dalle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative documentazioni.	Tutti	Ad evento
10	Le notizie relative a cambiamenti organizzativi (organigrammi)	Tutti	Ad evento
11	Gli aggiornamenti del sistema delle deleghe e dei poteri	Tutti	Ad evento
12	Mutamenti nelle situazioni di rischio o potenzialmente a rischio (es.: costituzione di "fondi a disposizione di organi aziendali")	Tutti	Ad evento
13	Le eventuali comunicazioni delle società di revisione riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni	Tutti	Ad evento
14	Copia dei verbali delle riunioni del Consiglio di Amministrazione	Tutti	Ad evento
15	Qualsiasi incarico conferito alla società di revisione o società ad esse collegate, diverso da quello concernente la revisione di bilancio	Tutti	Ad evento
16	Valutazioni in ordine alla scelta della società di revisione (in base ad elementi quali professionalità, esperienza nel settore, ecc., non solo in base a criteri di economicità)	Tutti	Ad evento
17	Qualunque informazione o notizia attinente alla commissione di reati previsti dal Decreto o comportamenti non in linea con il Modello predisposto	Tutti	Ad evento
18	Segnalazione di ogni violazione o sospetto di violazione del M.O. in forma anonima	Funzioni con attività di contatto con la PA	Ad evento

PARTE SPECIALE "A" - Processi Operativi e Strumentali				
Flussi verso OdV				
Tipologia di Informazioni		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	**Gestione verifiche ed ispezioni. Gestioni rapporti con PA** - Elenco delle contestazioni e dei contenziosi promossi dalla Pubblica Amministrazione.	Responsabile funzione delegata	Ad evento -	Parte speciale "A" - Processi operativi - Par. 1
2	**Obblighi Previdenziali -** Elenco delle irregolarità riscontrate, dell'elenco delle visite ispettive in corso e dell'elenco delle attività ispettive concluse	Responsabile funzione Risorse Umane/ Organizzazione	Ad evento	Parte speciale "A" - Processi operativi - Par. 3
3	**Selezione del Personale** - Elenco delle assunzioni effettuate in deroga al processo di selezione e/o a segnalazioni interne. . Elenco delle assunzioni di personale di paesi terzi.	Responsabile funzione Risorse Umane/ Organizzazione	Ad evento	Parte speciale "A" - Processi strumentali - Par. 1
4	**Finanza Dispositiva e Tesoreria** - Elenco dei: (1)Flussi Finanziari significativi rispetto al normale andamento del business, (2) Elenco dei flussi monetari e/o finanziari non standard realizzati nel periodo (operazioni straordinarie come sottoscrizioni e aumenti di capitale sociale, finanziamenti, cessioni di credito, operazioni in valuta estera e sui derivati - swap, futures, ecc.)	Responsabile Amministrazione e Finanza	Ad evento - Periodicità definita (sei mesi)	Parte speciale "A" - Processi strumentali - Par. 2
5	**Consulenze** - Consuntivo delle attività di consulenza /prestazioni professionali suddivise per consulente	Funzioni utilizzatrici o delegate a gestire il processo di acquisizione delle consulenze	Periodicità definita (sei mesi)	Parte speciale "A" - Processi Strumentali - Par. 3
6	**Gestione contenzioso e precontenzioso** - Elenco delle transazioni/sentenze significative (oltre un prestabilito valore soglia) e di quelle gestite in deroga.	Funzione operativa interessata	Periodicità definita (dodici mesi)	Parte speciale "A" - Processi strumentali - Par. 4

7	**Acquisti di Beni e Servizi** - Elenco degli acquisti effettuati in deroga ai requisiti di processo stabiliti	Acquisti	Ad evento -	Parte speciale "A" - Processi strumentali - Par. 5

PARTE SPECIALE "B" - Reati societari e di market abuse di cui agli artt. 25 ter e sexies				
Flussi verso OdV				
Tipologia di Informazioni		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione gestione e controllo
1	**False comunicazioni sociali e false comunicazioni sociali in danno dei soci e dei creditori** - Comunicazione di qualsiasi incarico conferito alla società di revisione o a società ad essa collegate, diverso da quello concernente la certificazione di bilancio	Vertice Aziendale	Sistematica	Parte Speciale "B"- Par. 7.1
2	**Falso in prospetto** - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Responsabile Amministrazione e Finanza	Ad evento	Parte Speciale "B"- Par. 7.2
3	**Falsità nelle relazioni e nelle comunicazioni alla società di revisione** - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale/ Responsabile Amministrazione e Finanza	Sistematica	Parte Speciale "B"- Par. 7.3
4	**Impedito Controllo** - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale	Su richiesta	Parte Speciale "B"- Par. 7.4
5	**Illecite operazioni sulle azioni proprie o quote sociali proprie o della società controllante**	Vertice Aziendale	Su richiesta	Parte Speciale "B"- Par. 7.5
6	**Operazioni in pregiudizio ai creditori** - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.6

7	**Omessa comunicazione del conflitto di interessi** - (1)Obbligo di comunicazione del proprio interesse in una determinata operazione e di astensione dalla decisione in materia; (2) Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Amministratori e Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.7
8	**Indebita restituzione dei conferimenti e illegale ripartizione degli utili o delle riserv**e - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.8
9	**Formazione fittizia del capitale** - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.9
10	**Illecita influenza sull'Assemble**a - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.10
11	**Abuso di informazioni privilegiate** - Informativa in merito agli obblighi giuridici e regolamentari che derivano dall'aver accesso a informazioni privilegiate	Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.11
12	**Manipolazione del mercato** - Segnalazione dei casi di irregolarità riscontrate nello svolgimento delle procedure di controllo	Vertice Aziendale	Ad evento	Parte Speciale "B"- Par. 7.12

PARTE SPECIALE "C" - Reati di omicidio colposo e lesioni gravi e gravissime in violazione degli adempimenti in materia di tutela della salute e della sicurezza sul lavoro, art. 25 septies				
Flussi verso OdV				
Tipologia di Informazioni		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	**Segnalazione aggiornamenti di documenti di valutazione del rischio**	Responsabile RSPP	Ad evento	Parte Speciale "C" - Par. 2.4
2	**Segnalazione sulla nomina delle cariche assegnate ai vari responsabili (RSPP, MC) e addetti a compiti speciali**	Responsabile RSPP	Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.4
3	**Segnalazione sull'aggiornamento dei certificati di prevenzione incendi e registro anticendi**	Responsabile RSPP	Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.4
4	**Segnalazione sull'aggiornamento della documentazione tecnico-procedurale**	Responsabile RSPP	Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.4
5	**Segnalazione dei casi di infortunio sul lavoro** (prima prognosi oltre 30gg.)	Responsabile RSPP	Ad evento	Parte Speciale "C" - Par. 2.4
6	**Comunicazione delle verifiche sulla sicurezza dei luoghi di lavoro effettuate da enti esterni**	Responsabile RSPP	Ad evento	Parte Speciale "C" - Par. 2.4

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "C" - Reati di omicidio colposo e lesioni gravi e gravissime in violazione degli adempimenti in materia di tutela della salute e della sicurezza sul lavoro, art. 25 septeis

Attività OdV

	Tipologia di Attività	Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà del Documento di valutazione del Rischio (DVR)	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
2	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà degli adempimenti formali previsti dalle procedure di controllo	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
3	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà di procedure di prevenzione degli incendi e gestione dell'emergenza	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
4	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà di attività di formazione	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
5	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà della documentazione procedurale	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
6	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà delle procedure di gestione dei contratti d'appalto e di prestazione d'opera	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
7	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà di procedure di sorveglianza sanitaria	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3
8	Verificare la sussistenza, la concreta ed effettiva rispondenza alla realtà della documentazione tecnica	Organismo di Vigilanza	Ad evento - Periodicità definita (annuale)	Parte Speciale "C" - Par. 2.3

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "D" - Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, art. 25 octies				
Flussi verso OdV				
Tipologia di Informazioni		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	**Segnalazione delle operazioni effettuate in deroga ai principi stabiliti nel Modello con riferimento a contratti di acquisto e/o di vendita con controparti (Rapporti con soggetti Terzi)**	Responsabile AF	Ad evento	Parte Speciale "D" - Par. 2 e 3.4
2	**Segnalazione delle operazioni effettuate in deroga ai principi stabiliti nel Modello con riferimento a transazioni finanziarie con controparti (Rapporti con soggetti Terzi)**	Responsabile AF	Ad evento	Parte Speciale "D" - Par. 2 e 3.4
3	**Segnalazione delle operazioni effettuate in deroga ai principi stabiliti nel Modello con riferimento a investimenti con controparti (Rapporti con soggetti Terzi)**	Vertice Aziendale	Ad evento	Parte Speciale "D" - Par. 2 e 3.4
4	**Segnalazione delle operazioni effettuate in deroga ai principi stabiliti nel Modello con riferimento a contratti infragruppo di acquisto e/o di vendita**	Responsabile AF	Ad evento	Parte Speciale "D" - Par. 2 e 3.4
5	**Segnalazione delle operazioni effettuate in deroga ai principi stabiliti nel Modello con riferimento alla gestione dei flussi finanziari**	Responsabile AF	Ad evento	Parte Speciale "D" - Par. 2 e 3.4
6	**Segnalazione delle operazioni effettuate in deroga ai principi stabiliti nel Modello con riferimento a investimenti Infragruppo**	Vertice Aziendale	Ad evento	Parte Speciale "D" - Par. 2 e 3.4

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "D" - Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, art. 25 octies				
Attività OdV				
	Tipologia di Attività	Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	Verifica dell'attendibilità commerciale e professionale dei fornitori e dei partner commerciali e finanziari	Società controllate/ Responsabile AF	Periodicità definita (semestrale)	Parte Speciale "D" - Par. 3.3
2	Controlli formali e sostanziali dei flussi finanziari aziendali	Responsabile AF	Periodicità definita (semestrale)	Parte Speciale "D" - Par. 3.3
3	Controllo dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard	Responsabile AF	Periodicità definita (semestrale)	Parte Speciale "D" - Par. 3.3
4	Verifica dell'adeguatezza della funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard	Responsabile funzioni operative	Periodicità definita (semestrale)	Parte Speciale "D" - Par. 3.3
5	Verifica dell'adeguatezza dell'identificazione di un organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti ruoli e responsabilità	Vertice aziendale	Periodicità definita (semestrale)	Parte Speciale "D" - Par. 3.3
6	Sovraintendere alla somministrazione di adeguati programmi di formazione ed informazione del personale ritenuto esposto al rischio di riciclaggio	Responsabile Risorse Umane/Organizzazione	Periodicità definita (semestrale)	Parte Speciale "D" - Par. 3.3
7	Comunicazione tempestiva al Consiglio di Amministrazione delle eventuali infrazioni della normativa in materia di riciclaggio	Vertice aziendale	Evento	Parte Speciale "D" - Par. 3.3

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "E" - Delitti informatici e trattamento illecito dei dati previsti dall'art. 24 bis del D. Lgs. 231/2001 (introdotto dalla Legge 48/2008)				
Flussi verso OdV				
Tipologia di Informazioni		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	**Comunicazione della piena conoscenza del processo da seguire e degli obblighi da osservare nello svolgimento dell'operazione, con dichiarazione di conformità al D. Lgs. 231/2001**	Responsabili di Funzione Sistemi Informativi	Ad evento	Parte speciale "E - Processi operativi - Par. 6
2	**Elencazione dei principali adempimenti effettuati nell'espletamento dell'attività di controllo e verifica**	Responsabili di Funzione Sistemi Informativi	Ad evento	Parte speciale "E - Processi operativi - Par. 6
3	**Comunicazione delle eventuali anomalie e deroghe di accesso ai sistemi informatici e telematici**	Responsabili di Funzione Sistemi Informativi	Ad evento	Parte speciale "E - Processi operativi - Par. 6

Macroaree di attività a rischio	
1	Sistemi informativi di Gestione aziendale
2	Servizi applicativi finanziario/gestionali
3	Elaborazione delle informazioni di carattere finanziario/gestionale
4	Attività di gestione, e/o amministrazione, e/o manutenzione dei sistemi IT
5	Sistemi informativi di supporto alla produzione

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "F" - Reati di criminalità organizzata e reati transnazionali				
Flussi verso OdV				
Tipologia di Informazioni		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	**Comunicazione di ogni fatto o elemento dal quale si possa desumere il rischio di interferenze/infiltrazioni criminali nelle attività aziendali, in riferimento ai reati di criminalità organizzata**	Destinatari del M.O.	Ad evento	Parte Speciale "F" - Par. 4.5
2	**Invio di flussi di segnalazione e di schede di evidenza inerenti ai processi di competenza,rientranti nell'ambito di rischio di reati di criminalità organizzata**	Destinatari del M.O.	Definite dal quadro procedurale aziendale	Parte Speciale "F" - Par. 4.5

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "F" - Reati di criminalità organizzata e reati transnazionali				
Attività OdV				
Tipologia di Attività		Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
1	**Verificare la validità di opportune clausole standard finalizzate:**			Parte Speciale "F" - Par. 4.4
1.a	**all'osservanza da parte dei collaboratori esterni e dei partner de contenuti del Modello e del Codice Etico**	Responsabili di primo livello di riporto al Vertice	Periodica (annuale)	
1.b	**alla possibilità di B.E.E. TEAM spa di effettuare efficaci azioni di controllo nei confronti dei destinatari del M.O.**	Responsabili di primo livello di riporto al Vertice	Periodica (annuale)	
1.c	**all'attuazione di meccanismi sanzionatori qualora si accertino violazioni nelle prescrizioni**	Responsabile RU	Periodica (annuale)	Parte Speciale "F" - Par. 4.4
2	**Verificare l'osservanza, attuazione ed adeguatezza del M.O. ai fini della prevenzione dei reati associativi**	Organismo di Vigilanza	Periodica (annuale)	Parte Speciale "F" - Par. 4.4
3	**Curare l'emanazione e l'aggiornamento di istruzioni standardizzate relative alla compilazione omogenea e coerente da parte dei responsabili interni:**			Parte Speciale "F" - Par. 4.4
3.a	**dei modelli di segnalazione periodica al Comitato di Controllo degli eventi a rischio di reato**	Responsabile RU	Periodica (annuale)	
3.b	**delle schede di evidenza del tracciamento delle attività a contatto con la PA**	Responsabile RU	Periodica (annuale)	

B.E.E. Team spa *–Tutti i diritti riservati.*

PARTE SPECIALE "G" - Reati di Abbandono ne e sul suolo di rifiuti ed acque reflue			
Flussi verso OdV			
Tipologia di Informazioni	Ente Responsabile	Tempistica	Riferimento nel documento di organizzazione, gestione e controllo
Elenco dei principali adempimenti effettuati nell'espletamento dell'attività di controllo e verifica da effettuarsi in particolare sui registri di carico e scarico, dichiarazione annuale e documenti di conferimento (formulari)	Servizi Generali	Annuale	Parte Speciale "G"

RISCHI RESIDUI

RISCHI RESIDUI

BEE TEAM CAPOGRUPPO

RD / PROCESSI	AMM	PERS	FIN DISPOS	MARK ABUSE	ISPEZ (PERS)	CONS (PERS)	RAPPR PERS	ACC. TR. (PERS)	PROC. GIUD. (PERS)	SICUREZZA
3100 - RC - COMPLIANCE D. LGS. 231 - ART. 24 - indebita percezione di erogazioni, truffa in danno dello Stato, frode informatica		BB							B	
3300 - RC - COMPLIANCE DLSG 231/01 art 24 ter associazioni a delinquere						BB		BB		
3400 - RC - COMPLIANCE D.LGS. 231 - ART. 25 - Corruzione e concussione	BB	BB	BB		B	BB	BB	BB	BB	
4000 - RC - COMPLIANCE D.LGS. 231 - ART. 25 octies - Antiriciclaggio			BB			BB				
4100 - RC. DLSG 231/01 - Delitti in materia di violazione diritti di autore						BB				
4500 - RC - D.LGS. 61- ART. 25 ter del D.Lgs.231 - REATI SOCIETARI	BB		BB							
4600 - RC - LEGGE 62/2005 - ART. 25 sexies del D. Lgs. 231 - Abusi di mercato	BB			BB						
4700 - RC - D.LGS. 81/2008 - ART. 25 septies del D.Lgs. 231 - Salute e sicurezza sui luoghi di lavoro										B

SEVERITÀ				
10	13	15	16
6	9	12	14
3	5	8	11
1	2	4	7

PROBABILITÀ

AA	14 15 16	altissimo
A	10 12 13	alto
MA	6 8 9 11	medio alto
MB	4 5 7	medio basso
B	2 3	basso
BB	1	bassissimo