



Modello di Organizzazione,
Gestione e Controllo ai sensi del
Decreto Legislativo 8 giugno 2001, n. 231

Approvato dall'Amministratore Unico di Techem S.r.l. in data 30 Giugno 2014

INDICE

| | |
|---|----|
| PREMESSA | 4 |
| DEFINIZIONI | 5 |
| 1. IL DECRETO LEGISLATIVO N. 231/2001 | 8 |
| 1.1 Caratteristiche fondamentali ed ambito di applicazione | |
| 1.2 Il Modello organizzativo come forma di esonero dalla responsabilità | |
| 1.3 L'apparato sanzionatorio | |
| 1.4 Linee guida di Confindustria | |
| 2. DESCRIZIONE DELLA REALTA' AZIENDALE – MODELLO DI GOVERNANCEE ASSETTO ORGANIZZATIVO DELLA SOCIETA' | 19 |
| 2.1 Techem S.r.l. | |
| 2.2 Il modello di governance di Techem S.r.l. | |
| 3. SCELTE DELLA SOCIETA' ED APPROCCIO METODOLOGICO | 22 |
| 3.1 Scelta di adottare il Modello di Organizzazione, Gestione e Controllo | |
| 3.2 Il processo di redazione ed implementazione del Modello 231/01 | |
| 3.3 Risk assessment ed individuazione dei reati | |
| 3.4 Stesura del Modello di Organizzazione, Gestione e Controllo | |
| 4. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI TECHEM S.R.L. | 27 |
| 4.1 Finalità del Modello di Organizzazione, Gestione e Controllo | |
| 4.2 Il Codice Etico | |
| 4.3 Destinatari del Modello di Organizzazione, Gestione e Controllo | |
| 4.4 Modifiche del Modello di Organizzazione, Gestione e Controllo | |
| 4.5 Diffusione del Modello di Organizzazione, Gestione e Controllo | |
| 5. L'ORGANISMO DI VIGILANZA AI SENSI DEL D.LGS. 231/2001 | 32 |

6. SISTEMA DISCIPLINARE.....33

- 6.1 Funzione del sistema disciplinare
- 6.2 Misure nei confronti dei dipendenti
- 6.3 Misure nei confronti dei dirigenti
- 6.4 Misure nei confronti degli Amministratori
- 6.5 Misure nei confronti dei collaboratori esterni, consulenti esterni, agenti, fornitori e appaltatori
- 6.6 Misure nei confronti di Membri dell'Organismo di Vigilanza

PARTE SPECIALE

7. I REATI37

- 7.1 Reati contro la Pubblica Amministrazione
- 7.2 Reati di criminalità informatica
- 7.3 Reati di criminalità organizzata
- 7.4 Reati contro l'industria e il commercio
- 7.5 Reati societari
- 7.6 Reati in tema di salute e sicurezza sul lavoro
- 7.7 Reati di ricettazione, riciclaggio ed impiego di denaro, beni ed utilità di provenienza illecita
- 7.8 Reati in violazione del diritto d'autore
- 7.9 Reato di impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare
- 7.10 Reati ambientali

ALLEGATI

- A. CODICE ETICO
- B. STATUTO DELL'ORGANO DI VIGILANZA

PREMESSA

Techem S.r.l., società leader a livello mondiale con oltre 60 anni di esperienza, esercita l'attività di commercio, installazione, manutenzione, riparazione, assistenza tecnica e noleggio di apparecchiature di supporto nel rilevamento e nella contabilizzazione di riscaldamento e acqua.

La Società, al fine di uniformarsi a quanto disposto dal d.lgs. 231/01e successive modifiche ed estensioni di applicabilità, nonché di garantire correttezza ed eticità nello svolgimento delle attività aziendali, ha ritenuto opportuno adottare un proprio Modello di Organizzazione e Controllo.

L'Amministratore Unico della Techem S.r.l. ha approvato in data 30 giugno 2014 il Modello di Organizzazione, Gestione e Controllo della Società ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della Legge 29 settembre 2000, n. 300", pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001. Contestualmente all'adozione del Modello, l'Amministratore Unico ha nominato un Organismo di Vigilanza a cui ha conferito i compiti di vigilanza e controllo previsti dal medesimo Decreto.

Il presente Modello si struttura in una Parte Generale ed in più Parti Speciali.

Nella Parte Generale viene descritto: il quadro normativo della 231/01 e successive modifiche; la realtà aziendale, governance ed assetto organizzativo di Techem S.r.l.; l'Organismo di Vigilanza, funzioni e poteri ad esso attribuite; struttura del Modello e sistema disciplinare adottato dalla Società.

Nelle Parti Speciali sono descritti, analiticamente, i Processi Sensibili ed i sistemi di controllo previsti da Techem S.r.l. al fine di prevenire il rischio di commissione di reati contemplati dal Decreto.

DEFINIZIONI

Nel presente documento e nei relativi allegati le seguenti espressioni hanno il significato di seguito indicato:

- **“Agenti”**: i soggetti che sono stabilmente incaricati dalla Società, in virtù di apposito contratto di agenzia, di promuovere la conclusione di contratti in una o più zone determinate.
- **“Appaltatori”**: Convenzionalmente si intendono tutti gli appaltatori di opere o di servizi ai sensi del codice civile, nonché i subappaltatori, i somministranti, i lavoratori autonomi che abbiano stipulato un contratto d’opera con la Società e di cui questa si avvale nei Processi Sensibili.
- **“Attività a rischio reato”**: operazione o atto che espone la Società al rischio di commissione di uno dei Reati contemplati dal Decreto.
- **“Casa madre”**: Techem Energy services G.M.B.H.
- **“CCNL”**: i Contratti Collettivi Nazionali di Lavoro applicati dalla Società.
- **“Codice Etico”**: documento contenente i principi generali di comportamento a cui destinatari devono attenersi anche con riferimento alle attività di cui al Modello di Organizzazione, Gestione e Controllo adottato dalla Società.
- **“Collaboratori”**: tutti i collaboratori, complessivamente considerati, legati da un rapporto contrattuale con Techem e di cui questa si avvale nei Processi Sensibili.
- **“Consulenti Esterni”**: i soggetti, non dipendenti di Techem, che agiscono in nome e/o per conto della Società in forza di un contratto di mandato o di altro rapporto contrattuale.
- **“D.Lgs. 231/2001”** o **“Decreto”**: Decreto Legislativo 8 giugno 2001, n. 231, recante la “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della Legge 29 settembre 2000, n. 300”, pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001 e successive modificazioni ed integrazioni.

- **“Destinatari”**: tutti i soggetti cui è rivolto il Modello e, in particolare: gli organi societari ed i loro componenti, i dipendenti, i fornitori, gli Agenti, i Consulenti Esterni, gli Appaltatori, i Collaboratori, nonché i membri dell’Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate.
- **“Dipendenti”** e **“Personale”**: i soggetti aventi un rapporto di lavoro subordinato o parasubordinato con la Società, ivi compresi i dirigenti.
- **“Fornitori”**: i fornitori di beni e servizi di cui la Techem si avvale nell’ambito dei “Processi Sensibili”.
- **“Linee Guida”**: le Linee Guida adottate da Confindustria per la predisposizione dei modelli di organizzazione, gestione e controllo ai sensi dell’art. 6, comma terzo, del D.Lgs. 231/2001.
- **“Manuale”**: Manuale di Gestione per la Qualità di Techem S.r.l..
- **“Modello”**: Modello di Organizzazione, Gestione e Controllo della Società che raccoglie l’insieme di processi e regole comportamentali che indirizzano lo svolgimento delle attività dell’Azienda in conformità alla legge che ha istituito la Responsabilità Amministrativa delle Persone Giuridiche (D.Lgs. 231/2001).
- **“Operazioni Sensibili”**: insieme di attività di particolare rilevanza svolte da Techem nei Processi Sensibili.
- **“Organismo di Vigilanza”** o **“ODV”**: Organismo previsto dall’art. 6 del D.Lgs. 231/2001, avente il compito di vigilare sul funzionamento e l’osservanza del Modello di Organizzazione, Gestione e Controllo.
- **“PA”**: la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio. Nell’ambito dei pubblici ufficiali ed incaricati di pubblico servizio sono ricompresi anche gli amministratori, i dirigenti ed i funzionari di società di diritto privato che svolgano un pubblico servizio.
- **“Processo sensibile”**: processo nel cui ambito ricorre il rischio di commissione dei reati; trattasi dei processi nelle cui fasi, sottofasi o attività si potrebbero in linea di

principio configurare le condizioni, le occasioni o i mezzi per la commissione di reati, anche in via strumentale alla concreta realizzazione della fattispecie di reato.

- **“Process Owner”**: il soggetto che per posizione organizzativa ricoperta o per le attività svolte è maggiormente coinvolto nel Processo Sensibile di riferimento.
- **“Procura”**: atto unilaterale con cui la Società attribuisce poteri di rappresentanza nei confronti di terzi.
- **“Reati”**: i reati ai quali si applica la disciplina prevista dal D.Lgs. 231/2001 (come modificato ed integrato in futuro).
- **“Responsabile Interno”**: soggetto interno alla Società al quale viene attribuita la responsabilità singola o condivisa con altri per le operazioni nelle Aree a Rischio.
- **“Sistema Disciplinare”**: insieme delle misure sanzionatorie applicabili in caso di violazione del Modello.
- **“Società”**: Techem s.r.l.

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/01

1.1 Caratteristiche fondamentali ed ambito di applicazione

Il D.Lgs. 231/2001 ha introdotto nell'ordinamento italiano la c.d. responsabilità "amministrativa" delle aziende, e, più in generale, degli enti, i quali possono essere chiamati a rispondere in sede penale per taluni reati, specificamente individuati dal legislatore. In particolare, perché l'azienda, o l'ente in generale, possano essere ritenuti responsabili ai sensi del D. Lgs. 231/01, è necessario che i reati siano commessi da soggetti che rivestono una posizione apicale all'interno dell'ente o azienda, od eventualmente anche da dipendenti dello stesso, e che, dalla commissione di tali reati, l'ente/azienda abbia tratto un proprio interesse o vantaggio. I reati individuati dal D. Lgs. 231/01 sono oltre cento, e vanno dai reati commessi ai danni della Pubblica Amministrazione, ai reati informatici, a quelli societari, ai delitti contro l'industria ed il commercio e a molti altri ancora. Questo elenco è, peraltro, in continuo aggiornamento, in quanto il legislatore tende sempre più ad allargare il novero delle fattispecie di reato contenute del D. Lgs. 231/01. In particolare con il recente D.Lgs. 121/2011 in attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della Direttiva 2009/123/CE sono stati aggiunti i reati ambientali. L'importanza dell'adeguamento a quanto previsto dalla 231/01 e successive modifiche è di fondamentale importanza per le imprese di qualunque dimensione e genere. La commissione di un illecito, può infatti riguardare le grandi aziende, le PMI, ma anche le microaziende. Gli effetti delle pesanti sanzioni pecuniarie nonché accessorie (es. sospensione o revoca licenza, accreditamento etc.) possono avere effetti devastanti. Al fine di ridurre il rischio di essere chiamati a rispondere per uno dei reati sanzionati dal D. Lgs. 231/01, le aziende hanno l'opportunità di adottare un Modello di organizzazione, gestione e controllo (c.d. Modello Organizzativo) con funzioni di prevenzione e contrasto dei reati sanzionati da tale norma. Il

D. Lgs. 231/01 prevede, inoltre, che il compito di vigilare sul funzionamento e l'osservanza dei Modelli Organizzativi, nonché quello di curare il loro aggiornamento, deve essere affidato ad un organismo, il c.d. Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e di controllo, la cui composizione può essere monocratica o collegiale.

La successiva legge 190/2012, c.d. "*statuto dell'anticorruzione*", ha affrontato il tema del contrasto alla corruzione in modo avvolgente, mettendo in atto tutte e tre le direttrici indicate in precedenza:

- aggravamento dell'impianto sanzionatorio previsto per questa tipologia di reati
- nuove ipotesi criminose di natura corruttiva nel sistema penale
- ampliamento dei reati di natura corruttiva che sono presupposto della responsabilità da reato per l'impresa.

Le innovazioni introdotte dalla legge anticorruzione (190/2012) hanno prodotto un forte impatto in entrambi gli ambiti pubblico e privato, vista la necessità - in questo secondo caso - di integrare il modello organizzativo in essere presso le aziende o, comunque, la necessità di dotarsi di un modello se non ancora in essere.

La disciplina anticorruzione contenuta nella legge 190/2012 comporta conseguenze rilevanti per le imprese che intendono adeguarsi al sistema di prevenzione previsto dal Dlgs 231/2001.

I nuovi reati che rilevano anche ai fini del D.Lgs. 231/2001 sono l'induzione indebita a dare o promettere utilità (art. 319-quater del Codice Penale) e la corruzione tra privati (art. 2635 del Codice Civile).

Nel primo caso potrà scattare la responsabilità della società, quando chi riveste funzioni di rappresentanza, amministrazione, direzione, gestione e controllo o un soggetto sottoposto alla loro direzione o vigilanza, materialmente dà, o promette, denaro o altra utilità al

pubblico ufficiale o all'incaricato di pubblico servizio. Questo comporta, in caso di accertata responsabilità, la condanna ad una sanzione pecuniaria oltre a misure interdittive.

Nel caso di corruzione tra privati, la responsabilità della società scatta quando un soggetto operante al suo interno ha agito per corrompere amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori.

La responsabilità delle "società" non opera "sic et simpliciter" per tutti i reati commessi da coloro che lavorano al loro interno, ma perché sussista occorre che siano integrati precisi elementi oggettivi e soggettivi (Art. 5 D.Lgs. 231/01)

Elementi oggettivi: deve, innanzitutto, trattarsi di reati specifici e, di seguito, verrà fornita una elencazione delle fattispecie - reato rilevanti:

- Reati in danno dello Stato o di altro Ente Pubblico (art. 24, D.Lgs.231/01).
- Delitti informatici e trattamento illecito di dati (art. 24-bis, D.Lgs. 231/01) [Articolo aggiunto dalla L. 18 marzo 2008 n. 48, art. 7]
- Delitti di criminalità organizzata (art. 24-ter, D.Lgs. 231/01) [Articolo aggiunto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29].
- Reati commessi nei rapporti con la Pubblica Amministrazione (art. 25, D.Lgs. 231/01) [Articolo modificato dalla L. 190/2012].
- Reati di falso nummario (art. 25-bis, D.Lgs. 231/01) [Articolo aggiunto dal D.L. 25settembre 2001 n. 350, art. 6, D.L. convertito con modificazioni dalla legge n. 409 del 23/11/2001; modificato dalla legge n. 99 del 23/07/09].
- Delitti contro l'industria e il commercio (art. 25-bis.1., D.Lgs. 231/01) [Articolo aggiunto dalla legge n. 99 del 23/07/09].
- Reati societari (art. 25-ter, D.Lgs. 231/01) [Articolo aggiunto dal D.Lgs. 11 aprile2002 n. 61, art. 3 e modificato dalla L. 190/2012].

- Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25-quater, D.Lgs. 231/01) [Articolo aggiunto dalla L. 14 gennaio 2003 n. 7, art. 3].
- Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.) (art. 25-quater.1, D.Lgs. 231/01) [Articolo aggiunto dalla L. 9 gennaio 2006 n. 7, art. 8].
- Delitti contro la personalità individuale (art. 25-quinquies, D.Lgs. 231/01) [Articolo aggiunto dalla L. 11/08/2003 n. 228, art. 5].
- Reati di abuso di mercato (art. 25-sexies, D.Lgs. 231/01) [Articolo aggiunto dalla L. 18 aprile 2005 n. 62, art. 9].
- Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinforturistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies, D.Lgs. 231/01) [Articolo aggiunto dalla L. 3 agosto 2007 n. 123, art. 9].
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies, D.Lgs. 231/01) [Articolo aggiunto dal D.Lgs. 21 novembre 2007 n. 231, art. 63, co. 3].
- Delitti in materia di violazione del diritto d'autore (art. 25-novies, D.Lgs. 231/01) [Articolo aggiunto dalla legge n. 99 del 23/07/09].
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-novies, D.Lgs. 231/01) [Articolo aggiunto dalla L. 3 agosto 2009n. 116, art. 4].
- Reati transnazionali (Legge 16 marzo 2006, n. 146, artt. 3 e 10).
- Reati ambientali (art. 25-undecies, D.Lgs. 231/01) [articolo aggiunto dal d.lgs. 121 del 7 luglio 2011].
- Impiego di cittadini terzi il cui soggiorno è irregolare (art. 25-duodecies, D.Lgs. 231/01)[articolo aggiunto dalla L. 190/2012]

Il reato deve, inoltre, essere commesso nell'interesse della società o a suo vantaggio.

Gli autori del reato devono essere persone fisiche che ricoprono una posizione apicale all'interno della società, oppure una posizione subordinata ai primi.

Gli autori del reato, infine, non devono aver agito nell'esclusivo interesse proprio o di terzi. Elementi Soggettivi: gli artt. 6 e 7 del D.lgs. 231/2001 pongono invece i criteri di natura soggettiva per la responsabilità della società. Il Legislatore, infatti, ha ritenuto che non fosse sufficiente una mera riconducibilità oggettiva del reato all'attività della società, ma che fosse anche necessaria una qualche forma di provvedimento specifico alla società stessa. Queste forme sono state individuate nel fatto che il reato si sia realizzato come espressione della politica aziendale, e quindi sia attribuibile ai soggetti in posizione apicale, oppure che il reato derivi da una colpa di organizzazione, e quindi sia attribuibile oggettivamente ai subordinati.

Qualora il reato sia stato commesso da un soggetto in posizione apicale all'interno della società, la legge presuppone che la commissione del reato sia espressione della politica d'impresa della società stessa e, quindi, ne presuppone la responsabilità, salvo prova contraria. Peraltro, non vi è solo un'inversione dell'onere della prova, ma la prova stessa è vincolata a specifici parametri. In altre parole, in questi casi è la società che deve fornire la prova della propria "innocenza".

Il processo a cui fa pertanto riferimento la norma, si articolerà, nella pratica, in due autonomi giudizi: uno nei confronti del collaboratore indagato ed un altro nei confronti dell'ente, con la possibilità di giungere, in caso di accertamento di un fatto corruttivo riconducibile all'ente (es.: prova del movimento contabile da un determinato conto a un altro), ad una condanna per la sola impresa che ne ha tratto vantaggio. Come evidenziato in precedenza, sono previste sanzioni pecuniarie ed eventualmente, per i casi più gravi, l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni funzionali alla commissione dell'illecito, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni o sussidi, il divieto di pubblicizzare beni o servizi, la confisca e pubblicazione della sentenza.

1.2 Il Modello organizzativo come forma di esonero dalla responsabilità

Il legislatore ha previsto la possibilità per la società di sottrarsi totalmente o parzialmente all'applicazione delle sanzioni, purché siano state rispettate determinate condizioni. L'art. 6 del Dlgs 231, infatti, contempla una forma di "esonero" da responsabilità dell'ente se si dimostra, in occasione di un procedimento penale per uno dei reati considerati, di aver adottato ed efficacemente attuato Modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati.

Il D.lgs. 231/01 differenzia i meccanismi di esonero dalla responsabilità a seconda che l'illecito sia commesso dai soggetti in posizione apicale o dai sottoposti. La prima situazione è disciplinata dal citato art. 6 del D.lgs. 231/01 ai sensi del quale la società può essere esonerata dalla responsabilità conseguente alla commissione dei reati indicati se prova che:

- a. l'Organo Dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi;
- b. il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo interno dotato di autonomi poteri di iniziativa e controllo;
- c. le persone fisiche hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- d. non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Qualora, viceversa, il reato sia commesso dai soggetti sottoposti all'altrui direzione o vigilanza, ai sensi dell'art. 7 del D.lgs. 231/01, la società è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.

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

Con l'adozione del Modello, naturalmente, non vi sono solo gli aspetti di tutela legale degli amministratori e dell'impresa, ma anche importanti vantaggi dal punto di vista dell'efficientamento dei processi interni, della trasparenza delle operazioni economiche e finanziarie e della capacità di intercettare richieste dal mercato.

1.3 L'apparato sanzionatorio

Le sanzioni previste dal Decreto si suddividono in:

- 1) amministrative pecuniarie;
- 2) interdittive;
- 3) confisca;
- 4) pubblicazione della sentenza.

La sanzione amministrativa pecuniaria è disciplinata agli artt. 10 e seguenti del decreto e costituisce la sanzione "base" nei confronti della società, che risponde con il suo patrimonio (art.27 "Responsabilità patrimoniale dell'ente").

Il Giudice, nell'irrogare la sanzione pecuniaria, ha l'obbligo di procedere a due diverse e successive operazioni di apprezzamento.

In un primo momento, il Giudice deve determinare il numero delle quote (in misura non inferiore a 100, né superiore a 1000- art.10), tenendo conto "della gravità del fatto, del grado della responsabilità della società nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti".

Dopodiché il Giudice determina il valore di ciascuna quota, da un minimo di Euro 258,22 ad un massimo di Euro 1.549,37.

Le sanzioni possono variare da un minimo di Euro 25.822,00 ad un massimo di Euro 1.549.370,00.

Ai fini della quantificazione delle quote il Giudice deve tenere conto:

- Della gravità del fatto
- Del grado di responsabilità della società
- Dell'attività svolta dalla società per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

L'importo della quota è fissato, invece, sulla base delle condizioni economiche e patrimoniali della società allo scopo di assicurare l'efficacia della sanzione (articoli 10 e 11).

Oltre a ciò, l'articolo 12 del decreto prevede una serie di casi in cui la sanzione pecuniaria viene ridotta (se l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato un vantaggio, o ne ha ricavato un vantaggio minimo; se il danno patrimoniale cagionato è di particolare tenuità; se la società, prima della dichiarazione di apertura del dibattimento di primo grado, ha risarcito integralmente il danno, ed ha eliminato le conseguenze dannose o pericolose del reato, ovvero si è comunque efficacemente adoperata in tal senso; se è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi).

Le sanzioni interdittive possono essere applicate solo in relazione ai reati per i quali sono espressamente previste dal decreto qualora ricorra, almeno, una delle seguenti condizioni:

- la società ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative";
- in caso di reiterazione degli illeciti.

Ai sensi del D.Lgs. 231/01 le sanzioni interdittive applicabili sono:

- interdizione temporanea o definitiva dall'esercizio dell'attività aziendale;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

- divieto di contrattare con la pubblica amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi;
- divieto temporaneo o definitivo di pubblicizzare beni o servizi.

L'interdizione dell'attività ha natura residuale rispetto alle altre sanzioni interdittive.

Infine, ai sensi dell'art.19, con la sentenza di condanna è sempre disposta la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede, nonché la pubblicazione della sentenza in presenza di una sanzione interdittiva a spese della società.

1.4 Linee Guida di Confindustria

Il più diffuso e riconosciuto riferimento per la redazione del Modello di Organizzazione, Gestione e Controllo, è rappresentato dalle Linee Guida di Confindustria.

Quest'ultima, in data 7 marzo 2002, ha approvato le prime "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.lgs. 231/2001", le quali sono state approvate dal Ministero della Giustizia nel giugno 2004. Il primo aggiornamento, sulla base anche dei rilievi sollevati dal Ministero, aveva riguardato, in particolare, l'ambito delle aree a rischio reato, i protocolli e l'Organismo di Vigilanza.

A seguito dei numerosi interventi legislativi che, nel frattempo, hanno modificato la disciplina della responsabilità amministrativa degli enti, estendendone l'ambito applicativo ad ulteriori fattispecie di reato nonché tenuto conto delle prime esperienze applicative realizzate dalle associazioni e dalle imprese, la Confindustria ha provveduto ad aggiornare al 31 marzo 2008 le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.lgs. 231/2001".

I punti fondamentali di tali Linee Guida possono essere così brevemente riassunti:

attività di individuazione delle aree a rischio, volta ad evidenziare le funzioni aziendali nell'ambito delle quali sia possibile la realizzazione degli eventi pregiudizievoli previsti dal Decreto; predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di appositi protocolli.

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

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

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

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

- autonomia ed indipendenza;
- professionalità ed onorabilità;
- continuità di azione;
- capacità specifiche in tema di attività ispettive e/o consulenziali.
- previsione di modalità di gestione delle risorse finanziarie;
- obblighi di informazione dell'Organismo di controllo.

Il mancato rispetto di punti specifici delle predette Linee Guida non inficia la validità del modello. Infatti, il modello adottato dall'Ente deve essere necessariamente redatto con specifico riferimento alla realtà concreta della società e, pertanto, lo stesso può anche

discostarsi dalle Linee Guida di Confindustria, le quali, per loro natura, hanno carattere generale.

Con riferimento ai reati societari, introdotti dal D.lgs. n. 61/2002, Confindustria ha precisato che è necessario approntare specifiche misure organizzative e procedurali (consistenti nel Modello) dirette a prevenire la commissione di tale tipologia di reati, nonché definire i principali compiti dell' organismo di Vigilanza per la verifica della effettività ed efficacia del Modello stesso.

2. DESCRIZIONE DELLA REALTA' AZIENDALE-MODELLO DI GOVERNANCE E ASSETTO ORGANIZZATIVO DELLA SOCIETA'

2.1 Techem S.r.l.

La Techem s.r.l. è una società di proprietà della Techem Energy services G.M.B.H. con sede in Germania . La casa madre fornisce alla Techem s.r.l. quasi tutti i prodotti (70%), le infrastrutture (call service, formazione, software e relativa assistenza). La Techem s.r.l. nasce nel 1995 ed è leader mondiale nel mercato delle apparecchiature di rilevamento radio installate. La casa madre è sul mercato da più di 55 anni ed è stata la prima società a:

- sviluppare la tecnologia relativa alla ripartizione di calore per sistemi di riscaldamento centralizzato nei condomini.
- Introdurre un modulo di regolazione ad onde-radio "enotech" che gestisce il flusso di calore prodotto dalla caldaia termica in funzione della quantità di calore richiesto dal singolo calorifero. I dati vengono trasmessi regolarmente ad "enotech" dal singolo ripartitore di calore Techem.

La società ha sede centrale in via dei Buonvisi 61D a Roma ed ha le filiali a Segrate (MI) in via G. Marconi n°6, a Rivoli (TO) in via Courgnè 36/b, a Brunico (BZ) in via Teodone 15/A ed è iscritta alla C.C.I.A.A. con numero di iscrizione 1484223.

La Techem è inoltre iscritta alla SOA dall'organismo di attestazione SOA LAGHI S.p.A., categoria 0528 con numero di iscrizione 3166/57/01.

L'attività direzionale e produttiva è svolta nella sede centrale, nelle filiali viene effettuato il processo produttivo.

L'obiettivo della Techem S.r.l. è quello di effettuare servizi fedeli alle aspettative dei clienti ed entro i tempi stabiliti dai contratti.

2.2 Il modello di governance ed assetto organizzativo di Techem S.r.l.

La Società è amministrata da un Amministratore Unico.

L'organo amministrativo è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società ed in particolare sono riconosciute ad esso tutte le facoltà per l'attuazione dell'oggetto sociale, che non siano dalla legge o dallo statuto, in modo tassativo, riservate all'assemblea dei soci.

La revisione legale di cui al D.lgs. 39/2010 spetta, invece, ai revisori contabili iscritti nel registro istituito presso il Ministero della Giustizia.

La Techem S.r.l., allo scopo di definire, descrivere e regolamentare tutte le attività necessarie per implementare un efficace Sistema di Gestione per la Qualità in accordo alla norma UNI EN ISO 9001:2008 all'interno della società, si è dotata di un Manuale di Gestione per la Qualità.

Il Sistema di Gestione per la Qualità è stato attuato attraverso un approccio per processi. ed ha determinato i seguenti processi, necessari per il Sistema stesso e la loro applicazione nell'ambito di tutta l'organizzazione:

Processi operativi primari:

- COMMERCIALE (acquisizione commesse, aggiudicazione gare)
- PIANIFICAZIONE
- APPROVVIGIONAMENTO
- INSTALLAZIONE
- CONTABILIZZAZIONE CONSUMI

Processi operativi di supporto:

- GESTIONE DELLE RISORSE

Processi gestionali:

- TENUTA SOTTO CONTROLLO DEI DOCUMENTI
- TENUTA SOTTO CONTROLLO DELLE REGISTRAZIONI
- VERIFICHE ISPETTIVE
- TENUTA SOTTO CONTROLLO DEI PRODOTTI NON CONFORMI
- MIGLIORAMENTO CONTINUO
- AZIONI CORRETTIVE E PREVENTIVE

I suddetti processi sono stati sviluppati nel Manuale in Procedure, Istruzioni di lavoro, Piani di qualità, Moduli e Schede.

Il controllo dei processi è garantito dall'applicazione della suddetta documentazione.

La disponibilità delle informazioni necessarie a supportare l'attuazione e il monitoraggio dei processi è garantita dall'organizzazione aziendale e dalle relative responsabilità descritte nel Manuale.

I processi sono misurati, monitorati e analizzati secondo le modalità descritte nel Manuale. Tutti i processi sopra indicati sono finalizzati alla soddisfazione del cliente e ad una efficiente gestione della Techem S.r.l., nel rispetto di tutte le prescrizioni cogenti e delle leggi in vigore.

La società Techem attua le azioni necessarie per migliorare il prodotto offerto attraverso attività di verifica ispettiva interna, prevenzione e correzione delle non conformità.

Nell'ambito della propria attività d'impresa, la Techem S.r.l. affida alcune lavorazioni a fornitori di servizi opportunamente valutati e quindi ritenuti idonei allo scopo.

Anche in tali casi il controllo del processo produttivo del fornitore di servizi viene attuato seguendo le modalità precedentemente descritte.

3. SCELTE DELLA SOCIETA' ED APPROCCIO METODOLOGICO

3.1 Scelta di adottare il Modello di Organizzazione, Gestione e controllo

Techem S.r.l., alla luce della volontà di operare in modo trasparente e corretto, anche a presidio della propria reputazione aziendale, così come dei propri soci, amministratori e dipendenti, ha ritenuto opportuno, in linea con la filosofia aziendale, procedere all'adozione e all'attuazione di un Modello di Organizzazione Gestione e Controllo ai sensi del D.Lgs. 8 giugno 2001 n. 231, stabilendo, altresì, di procedere ad un suo costante aggiornamento.

Sino all'adozione del Modello, comunque, la società, adottava procedure tese alla più ampia trasparenza delle attività svolte nonché alla prevenzione di eventi delittuosi da parte di amministratori o dipendenti.

In particolare ed a titolo di esempio si riportano le procedure adottate nei settori di particolare sensibilità:

TESORERIA

La procedura, considerevolmente rigida, prevede che ogni bonifico abbia una doppia firma di autorizzazione, che ogni bonifico avvenga a seguito di una autorizzazione scritta al pagamento dal capoarea e che l'impiegato addetto ai pagamenti non sia la stessa persona che registra la contabilità; che non venga gestito contante e che tutti i pagamenti e gli incassi avvengano tramite bonifici o assegni.

ACQUISTI

- tutti gli acquisti (o i contratti nel caso di consulenti) devono essere basati su preventivi multipli;
- tutti gli acquisti devono essere vagliati dal gestionale evitando così arbitrarietà;
- A tutti i fornitori viene richiesta la tracciabilità finanziaria;

VENDITE

- contratti di procacceria a norma di legge con definizione percentuali e condizioni;
- convenzioni a norma di legge con definizione percentuali e condizioni.

Techem S.r.l., nell'ottica di una incentivazione e sensibilizzazione di una cultura aziendale improntata alla prevenzione del rischio di reati, oltre che alla valorizzazione di un'etica orientata alla correttezza e trasparenza nella conduzione degli affari, ha, quindi, avviato un progetto di analisi ed adeguamento a quanto previsto dal Decreto dei propri strumenti organizzativi, di gestione e controllo.

L'adozione del Modello costituisce il punto di partenza di un processo di sensibilizzazione di tutti coloro che operano per conto della Società. Come chiarito dalle Linee Guida di Confindustria, l'organo amministrativo di Techem, pur con l'istituzione dell'Organismo di Vigilanza ai sensi del Decreto, mantiene invariate tutte le attribuzioni e responsabilità previste dal Codice Civile e dallo Statuto, alle quali oggi si aggiungono quelle relative all'efficace attuazione del Modello nonché al funzionamento dell'Organismo stesso. In ogni caso, la corretta attuazione e il controllo delle regole contenute nel Modello, costituiscono, quindi, un obbligo e un dovere di tutto il personale della società e, in particolare, di ciascun responsabile di funzione cui è demandata, nell'ambito di propria competenza, la responsabilità primaria sul controllo delle attività, specialmente di quelle a rischio.

3.2 Il processo di redazione ed implementazione del Modello 231/2001

Di seguito si riportano le fasi essenziali dell'approccio metodologico adottato da Techem S.r.l. per la conduzione del processo di redazione ed implementazione del Modello 231/2001:

- Fase preliminare

In tale fase, finalizzata alla pianificazione delle attività di rilevazione, sono state condotte analisi puntuali sulla documentazione esistente (statuto, organigrammi, Manuale di Gestione per la Qualità ecc.) e confronti con le funzioni aziendali interessate, allo scopo di identificare i soggetti apicali e sottoposti da coinvolgere nella successiva fase di valutazione dei rischi e del sistema dei controlli. Sono state individuate le aree di attività nelle quali esiste il rischio di commissione dei reati

previsti dal Decreto e, allo scopo di facilitare la successiva fase di valutazione dei rischi, sono state identificate le possibili modalità di conduzione della condotta illecita.

- Fase di mappatura dei rischi e dei controlli

In tale fase, tenuto conto di quanto suggerito dalle Linee Guida, si è proceduto ad una approfondita indagine della complessiva organizzazione della Società, ovvero una ricognizione delle aree, dei settori e degli uffici, delle relative funzioni e procedure e delle entità esterne in vario modo correlate con la società stessa. Per ciascuna di tali aree sono state condotte puntuali analisi documentali ed interviste alle figure apicali e sottoposte coinvolte nelle attività esaminate, per identificare i reati che potenzialmente potrebbero essere commessi, le concrete modalità di commissione, la natura dei controlli esistenti (ad es. quelli di tipo organizzativo; quelli di tipo procedurale, connessi alla formalizzazione delle attività in regole interne). La fase di rilevazione dei rischi e dei controlli ha consentito di pervenire alla ricostruzione di un dettaglio delle aree aziendali “sensibili”, con identificazione delle funzioni e dei soggetti coinvolti e della loro responsabilità nonché dei sistemi di controllo adottati per la mitigazione dei rischi.

- Fase di valutazione dei rischi e dei controlli

In tale fase si è provveduto, per ciascuno dei processi sensibili, alla valutazione del grado di rischiosità, individuando le opportune azioni correttive per migliorare il sistema dei controlli e ridurre il livello di criticità.

- Fase di condivisione con il Management

Affinché il processo di revisione e aggiornamento della Mappatura delle aree a rischio e dei controlli potesse rappresentare una reale occasione di sensibilizzazione e coinvolgimento, l'intero processo valutativo e le relative evidenze emerse sono state condivise con il management interessato.

3.3 Risk assessment ed individuazione dei reati

L'analisi e la valutazione di risk assessment si è incentrata sulla definizione delle singole fattispecie di reato associabili a ciascuna area organizzativa della Società.

In secondo luogo si è proceduto ad effettuare un'analisi comparativa (la c.d. "gap analysis") tra il modello organizzativo e di controllo esistente ed un astratto modello di riferimento valutato sulla base del contenuto della disciplina di cui al D.Lgs. n. 231/2001.

Attraverso il confronto operato con la gap analysis è stato possibile desumere aree di miglioramento del sistema di controllo interno esistente e, sulla scorta di quanto emerso, è stato predisposto un piano di attuazione teso ad individuare i requisiti organizzativi caratterizzanti un modello di organizzazione, gestione e controllo conforme a quanto disposto dal D.Lgs. n. 231/2001 e le azioni di miglioramento del sistema di controllo interno. Le finalità che hanno caratterizzato questa fase di analisi sono:

- Individuazione delle fattispecie di reato associabili a ciascuna Unità Operativa
- Riduzione della possibilità di commettere reato
- Mantenimento, per quanto possibile, con opportune modifiche, ove necessario, la struttura di controllo esistente rendendola più efficiente ed efficace, garantendo, così, il giusto equilibrio tra controlli e linearità del processo decisionale con un attento sguardo al carico di lavoro delle singole Unità Operative.

Le fattispecie reato individuate con l'analisi e la valutazione di risk assessment effettuata sono le seguenti:

- Reati commessi nei rapporti con la Pubblica Amministrazione (art. 25, D.Lgs. 231/01) [Articolo modificato dalla L. 190/2012].
- Delitti informatici e trattamento illecito di dati (art. 24-bis, D.Lgs. 231/01) [Articolo aggiunto dalla L. 18 marzo 2008 n. 48, art. 7].
- Delitti di criminalità organizzata (art. 24-ter, D.Lgs. 231/01) [Articolo aggiunto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29].

- Delitti contro l'industria e il commercio (art. 25-bis.1., D.Lgs. 231/01) [Articolo aggiunto dalla legge n. 99 del 23/07/09].
- Reati societari (art. 25-ter, D.Lgs. 231/01) [Articolo aggiunto dal D.Lgs. 11 aprile 2002 n. 61, art. 3 e modificato dalla L. 190/2012].
- Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies, D.Lgs. 231/01) [Articolo aggiunto dalla L. 3 agosto 2007 n. 123, art. 9].
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies, D.Lgs. 231/01) [Articolo aggiunto dal D.Lgs. 21 novembre 2007 n. 231, art. 63, co. 3].
- Delitti in materia di violazione del diritto d'autore (art. 25-novies, D.Lgs. 231/01) [Articolo aggiunto dalla legge n. 99 del 23/07/09].
- Reati ambientali (art. 25-undecies, D.Lgs. 231/01) [articolo aggiunto dal D.Lgs. 121 del 7 luglio 2011].
- Impiego di cittadini terzi il cui soggiorno è irregolare (art. 25-duodecies, D.Lgs. 231/01)[articolo aggiunto dalla L. 190/2012].

La documentazione predisposta nell'ambito dell'attività di risk assessment per fattispecie di reato, al fine di effettuare la valutazione sulle criticità presenti nell'organizzazione societaria, è disponibile presso l'Archivio.

Le singole fattispecie di reato verranno trattate in apposita Parte Speciale del Modello.

3.4 Stesura del Modello di Organizzazione, Gestione e Controllo

A seguito di attenta analisi del rischio, dopo aver condiviso le risultanze con il Management della Società, si è, quindi, proceduto alla stesura del Modello 231/01.

Il Modello è stato approvato in data 16 giugno 2014 dall'Amministratore Unico, Dott. Octavio Manuel Prieto Izaguirre.

4. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI TECHEM S.R.L.

4.1 Finalità del Modello di Organizzazione, Gestione Finalità del Modello e Controllo

Il Modello, così come approvato, comprende i seguenti elementi costitutivi:

- Processo di individuazione delle attività aziendali nel cui ambito possono essere commessi reati richiamati dal D.Lgs. n. 231/2001
- Previsione di protocolli (o standard) di controllo in relazione alle attività sensibili individuate
- Processo di individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati
- Organismo di vigilanza
- Flussi informativi da e verso l'organismo di vigilanza e specifici obblighi di informazione nei confronti dell'organismo di vigilanza
- Sistema disciplinare atto a sanzionare la violazione delle disposizioni contenute nel Modello
- Piano di formazione e comunicazione al personale dipendente e ad altri soggetti che interagiscono con la Società
- Criteri di aggiornamento e adeguamento del Modello
- Codice Etico.

I sopra citati elementi costitutivi sono rappresentati nei seguenti documenti:

- Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01. Contiene: una Parte Generale costituita dal quadro normativo; realtà aziendale, modello di governance e assetto organizzativo; nomina, caratteristiche, funzioni ed obblighi dell'Organismo di Vigilanza; Sistema disciplinare; piano di formazione; criteri di aggiornamento ed adeguamento alla normativa in materia del Modello. Una Parte Speciale costituita dalle singole fattispecie reato individuate.

- Codice Etico. È parte integrante del Modello ed è approvato, unitamente ad esso, dall'Amministratore Unico. Raccoglie i principi etici ed i valori che informano la cultura aziendale ed esprime impegni e responsabilità etiche nella conduzione degli affari.

4.2 Il Codice Etico

La Società impone a tutto il personale di rispettare i principi comportamentali contenuti nel Codice Etico elaborato specificamente per coprire interamente l'ambito degli obblighi comportamentali da imporre ai sensi del D.Lgs. 231/2001.

Va, quindi, segnalato che il Codice Etico riveste una portata generale in quanto contiene una serie di principi di "deontologia aziendale", che la Società riconosce come propri e sui quali intende richiamare l'osservanza di tutti i suoi dipendenti e di tutti coloro che, anche all'esterno della Società, cooperano al perseguimento dei fini aziendali. La Società ha già svolto un'opera di puntuale ed effettiva diffusione, al suo interno e nei confronti dei soggetti che con essa collaborano, delle informazioni relative alla disciplina normativa ed alle regole comportamentali e procedurali da rispettare, al fine di assicurare che l'attività d'impresa si svolga nel rispetto dei principi etici di Techem S.r.l..

In ogni caso, si ritiene opportuno, anche in relazione alle speciali previsioni del Decreto, dare ulteriore impulso alla circolazione ed alla comprensione, da parte di tutti i soggetti interessati, delle norme di legge e dei canoni etici che orientano l'operato societario.

Il Codice Etico, inoltre, sarà sottoposto a verifica e sarà periodicamente oggetto di monitoraggio e adeguamento sia con riferimento alle novità legislative, sia per effetto delle vicende modificative dell'operatività della Società e/o della sua organizzazione interna.

I principi e le disposizioni del Codice Etico sono vincolanti per gli amministratori, i dipendenti e tutti coloro che operano con la Società sulla base di un rapporto contrattuale, anche temporaneo.

In particolare l'Amministratore Unico è tenuto ad ispirarsi ai principi del Codice, nel fissare gli obiettivi della Società, nel proporre gli investimenti e realizzare i progetti, nonché in qualsiasi decisione o azione relativa alla gestione della Società;

del pari i dirigenti, nel dare concreta attuazione all'attività di direzione della Società, dovranno ispirarsi ai medesimi principi, sia all'interno della Società, rafforzando così la coesione e lo spirito di reciproca collaborazione tra tutti coloro che operano in Azienda, sia nei confronti dei terzi che entrano in contatto con la Società stessa.

I dipendenti ed i collaboratori non subordinati della Techem e tutti coloro che intrattengono rapporti contrattuali di lungo periodo con essa, sono tenuti ad adeguare i propri comportamenti alle disposizioni del Codice Etico.

Allo scopo di assicurare la corretta comprensione del Codice Etico, vengono predisposti e realizzati piani periodici di comunicazione volti a favorire la conoscenza dei principi e delle norme etiche contenuti nel Codice Etico.

4.3 Destinatari del Modello di Organizzazione, Gestione e Controllo

Il Modello redatto da Techem S.r.l. è destinato a tutti coloro che operano a qualsiasi titolo o ragione in nome e per conto della stessa, indipendentemente dalla tipologia di rapporto instaurato.

In particolare le prescrizioni del Modello sono indirizzate agli Organi Societari ed ai loro componenti che rivestono funzioni di rappresentanza, amministrazione, direzione o controllo della Società ed a tutti coloro che sono sottoposti alla loro direzione o vigilanza, agli agenti, ai fornitori, ai consulenti esterni, agli appaltatori, nonché ai membri dell'Organismo di Vigilanza se non appartenenti ad altra categoria.

A coloro che, pur operando all'esterno della società ne abbiamo accettato il contenuto e gli effetti in virtù di specifiche clausole contrattuali e limitatamente allo svolgimento delle attività cui gli stessi sono preposti.

4.4 Modifiche del Modello di Organizzazione, Gestione e Controllo

Essendo il Modello un “atto di emanazione dell’organo dirigente”, in conformità alle prescrizioni dell’art. 6, comma i, lettera a) del Decreto, le successive modifiche e integrazioni sono rimesse alla competenza dell’Amministratore Unico.

L’Amministratore Unico di Techem S.r.l., con l’ausilio dell’Organismo di Vigilanza della stessa, provvede a comunicare tempestivamente ai Soggetti di cui al capo 4.3, le modifiche apportate al presente Modello.

Ogni modifica apportata al presente Modello dovrà essere, tempestivamente, comunicata all’ODV che ne vaglierà la conformità ai Principi Generali ed al Codice Etico nonché ad ogni Parte del presente Modello.

Fra le modifiche di carattere sostanziale rientrano a titolo di esemplificativo e non esaustivo:

- Aggiunta di ulteriori Parti Speciali
- Soppressione di parti del Modello
- Modifica della composizione e/o compiti dell’ODV
- Aggiornamento e/o modifica e/o integrazione di ogni parte del presente Modello.

4.5 Diffusione del Modello di Organizzazione, Gestione e Controllo

Ai fini dell’efficacia del presente Modello è necessaria una capillare diffusione dello stesso in ogni sua Parte, in particolare delle regole di condotta in esso contenute, tra le Risorse già presenti in Azienda sia di quelle che ne entreranno a far parte in futuro.

Il grado di approfondimento sarà correlato al grado di coinvolgimento nei Processi Sensibili.

Al fine di garantire l’effettiva conoscenza del Modello, una volta che è stato diffuso e consegnato, e sensibilizzato il personale sul rispetto della normativa e sull’osservanza dei principi e delle procedure in esso contenute, devono essere previste specifiche attività formative definite all’interno di apposito e organico piano formativo. Tale Piano dovrà essere articolato attraverso specifiche attività (ad esempio, corsi e seminari) a cui è posto l’obbligo di partecipazione. Tali iniziative dovranno essere differenziate, in relazione ai contenuti e alle modalità di diffusione, in funzione della qualifica dei destinatari, del livello

di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società. È compito dell'Organismo di Vigilanza pianificare adeguatamente, con la funzione aziendale preposta, l'attività di formazione dei dipendenti, del management e degli Esterni sui contenuti del Codice Etico, del Modello e delle relative procedure operative, sulle modalità di attuazione ad esse relative, sul livello di rischio di ogni singola area e sul sistema sanzionatorio previsto in caso di mancata osservanza dei suddetti documenti di governance aziendali. È compito dell'Organismo di Vigilanza verificare la completa attuazione del piano di formazione, raccogliere le evidenze relative all'effettiva partecipazione ai corsi e conservarle negli appositi archivi, nonché effettuare controlli periodici sul grado di conoscenza da parte dei dipendenti del D. Lgs. 231/2001, del Modello e delle procedure aziendali.

5. L'ORGANISMO DI VIGILANZA AI SENSI DEL D.LGS. 231/2001

In ottemperanza a quanto previsto all'art. 6, lettera b), del D.lgs. 231/01, viene istituito presso la Techem S.r.l. un organo con funzioni di vigilanza e controllo in ordine al funzionamento, all'efficacia, all'adeguatezza ed all'osservanza del Modello.

Nell'esercizio delle sue funzioni, l'Organismo di Vigilanza e Controllo deve improntarsi a principi di autonomia ed indipendenza. Esso deve riportare direttamente all'Amministratore Unico.

Unitamente al presente Modello l'Amministratore Unico di Techem S.r.l. approva lo Statuto dell'Organismo di Vigilanza da considerarsi parte integrante del presente documento al quale viene allegato ed al quale si rimanda per principi, funzioni, poteri ed obblighi dell'ODV.

6. SISTEMA DISCIPLINARE

6.1 Funzione del sistema disciplinare

La definizione di un sistema di sanzioni applicabili in caso di violazione delle regole di cui al Modello, rende efficiente l'azione di controllo dell'Organismo di Vigilanza ed ha lo scopo di garantirne l'effettività.

La definizione di tale sistema disciplinare costituisce, infatti, ai sensi dell'art. 6, comma 1, lett. e) del D.Lgs. 231/2001, un requisito essenziale ai fini dell'esimente rispetto alla responsabilità della Società. L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D.Lgs. n. 231/2001 indicano, quale condizione per un'efficace attuazione del modello di organizzazione, gestione e controllo, l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello stesso.

Tale sistema sanzionatorio si rivolge ai dirigenti, ai dipendenti, e agli amministratori, prevedendo adeguate sanzioni di carattere disciplinare.

Pertanto, la definizione di un adeguato sistema disciplinare costituisce un presupposto essenziale della valenza scriminante del modello rispetto alla responsabilità amministrativa delle società.

L'adozione di provvedimenti disciplinari in ipotesi di violazioni alle disposizioni contenute nel Modello prescinde dalla commissione di un reato e dallo svolgimento e dall'esito del procedimento penale eventualmente instaurato dall'Autorità Giudiziaria. L'osservanza delle prescrizioni contenute nel Modello adottato dalla Società deve considerarsi parte essenziale delle obbligazioni contrattuali dei destinatari dello stesso.

Il mancato rispetto e/o la violazione dei principi generali del Modello, delle regole di comportamento imposte dal Codice etico, dal Sistema disciplinare e dalle procedure aziendali, ad opera di lavoratori dipendenti della Società, costituiranno inadempimento alle obbligazioni derivanti da rapporto di lavoro ed illecito disciplinare.

Nei casi giudicati più gravi, la violazione può comportare la risoluzione del rapporto di lavoro, se posta in essere da un dipendente, ovvero all'interruzione del rapporto, se posta in essere da un soggetto terzo.

Fermo restando il principio di collegamento tra i provvedimenti disciplinari irrogabili e le fattispecie in relazione alle quali gli stessi possono essere assunti, nell'irrogazione della sanzione disciplinare dovrà necessariamente essere rispettato il principio della proporzionalità tra infrazione e sanzione.

Ciascun destinatario del presente Modello dovrà, quindi, necessariamente conoscere le norme contenute nello stesso, oltre le norme di riferimento che regolano l'attività svolta nell'ambito della propria funzione.

Con riguardo ai lavoratori dipendenti, il Decreto prevede che il sistema disciplinare debba rispettare i limiti connessi al potere sanzionatorio imposti dall'art. 7 della L. n. 300/1970 (c.d. "Statuto dei lavoratori") e dalla contrattualizzazione collettiva di settore e aziendale, sia per quanto riguarda le sanzioni irrogabili (che in linea di principio risultano "tipizzate" in relazione al collegamento con specificati indebiti disciplinari) sia per quanto riguarda la forma di esercizio di tale potere. Con riferimento alle sanzioni irrogabili, si precisa che esse dovranno essere adottate ed applicate nel rispetto delle procedure previste dalle normative collettive nazionali ed aziendali applicabili al rapporto di lavoro.

Il sistema sanzionatorio e le sue applicazioni vengono costantemente monitorati dall'Organismo di Vigilanza.

Nessun procedimento disciplinare potrà essere archiviato, né alcuna sanzione disciplinare potrà essere irrogata, per violazione del presente Modello, senza preventiva informazione e parere dell'Organismo di Vigilanza.

6.2 Misure nei confronti dei dipendenti

Il Modello di Organizzazione, Gestione e Controllo ed il Codice Etico costituiscono un complesso di norme alle quali il personale dipendente di una società deve uniformarsi

anche ai sensi di quanto previsto dagli artt. 2104 e 2106 c.c. e dai CCNL in materia di norme comportamentali e di sanzioni disciplinari.

Tutti i comportamenti tenuti dai dipendenti in violazione delle previsioni del Codice Etico, del Modello e delle sue procedure di attuazione, costituiscono inadempimento alle obbligazioni primarie del rapporto di lavoro e, conseguentemente, infrazioni, comportanti la possibilità dell'instaurazione di un procedimento disciplinare e la conseguente applicazione delle relative sanzioni.

6.3 Misure nei confronti dei dirigenti

Per quanto attiene le violazioni poste in essere dai dipendenti della Società con la qualifica di dirigente anch'esse costituiscono illecito disciplinare.

Il rapporto tra organo dirigenziale e l'azienda si caratterizza per la natura eminentemente fiduciaria. Il comportamento dei dirigenti costituisce esempio per tutti coloro che operano all'interno della realtà aziendale e si ripercuote sull'immagine esterna della stessa. Il rispetto da parte dei dirigenti, quindi, di ogni prescrizione contenuta nel Codice Etico, nel Modello e nelle relative procedure di attuazione costituisce elemento essenziale del rapporto di lavoro dirigenziale.

Nei confronti dei Dirigenti che abbiano commesso una violazione del Codice Etico, del Modello o delle procedure stabilite in attuazione del medesimo, viene avviato il procedimento disciplinare con l'effettuazione delle relative contestazioni e applicazione delle misure sanzionatorie più idonee, in conformità con quanto previsto dal CCNL Dirigenti e, ove necessario, con l'osservanza delle procedure di cui all'art. 7 della L. 300/1970.

Le sanzioni devono essere applicate nel rispetto dei principi di gradualità e proporzionalità rispetto alla gravità del fatto e della colpa o dell'eventuale dolo.

6.4 Misure nei confronti degli amministratori

Techem valuta con estremo rigore ogni violazione del presente Modello realizzata da coloro che ricoprono ruoli di vertice in seno alla Società, e che, per tale ragione, sono più in grado

di orientare l'etica aziendale e l'operato di chi opera nella Società ai valori di correttezza, legalità e trasparenza.

Anche, e soprattutto per i motivi dedotti, nei confronti degli Amministratori che abbiano commesso una violazione del Codice Etico, del Modello o delle procedure stabilite in attuazione del medesimo, l'Amministratore Unico oppure, ove occorra, l'Assemblea dei Soci, può applicare, nel rispetto dei principi di gradualità e proporzionalità rispetto alla gravità del fatto e della colpa o dell'eventuale dolo, ogni idoneo provvedimento consentito dalla legge.

6.5 Misure nei confronti dei collaboratori esterni, consulenti esterni, agenti, fornitori e appaltatori

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

Qualora si verifichi una violazione da parte di questi soggetti, l'ODV informa, con relazione l'Amministratore Unico.

6.6 Misure nei confronti di membri dell'Organismo di Vigilanza

Per i provvedimenti nei confronti dei membri dell'Organismo di Vigilanza, si rimanda alla disciplina di revoca dall'incarico dettata per gli stessi

PARTE SPECIALE

7. I REATI

7.1 Reati contro la Pubblica Amministrazione

Tra i reati nei confronti della Pubblica Amministrazione previsti dal Decreto si evidenziano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da Techem:

- Corruzione per l'esercizio della funzione (art. 318 c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o dipendente della Società prometta o dia a un Pubblico Ufficiale, per sé o per altri, una retribuzione che non gli è dovuta, sotto forma di denaro o altra utilità per esercitare ovvero per avere esercitato la propria funzione od i suoi poteri. Il reato si configura sia nei confronti del corrotto che del corruttore.
- Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o dipendente della Società dia o prometta a un Pubblico Ufficiale, per sé o per altri, denaro o altra utilità per omettere o ritardare, per avere omesso o ritardato, un atto del suo ufficio, ovvero per compiere o per avere compiuto un atto contrario ai doveri di ufficio. Il reato si configura sia nei confronti del corrotto che del corruttore.
- Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.) – Tale ipotesi di reato si configura nel caso in cui la corruzione per un atto d'ufficio o per un atto contrario ai doveri di ufficio riguardino un Incaricato di Pubblico Servizio.
- Istigazione alla corruzione (art. 322 c.p.) – Tale ipotesi di reato si configura nel caso in cui il dipendente o rappresentante della Società offra denaro o altra utilità a un Pubblico Ufficiale o ad un Incaricato di Pubblico Servizio per una finalità corruttiva ma l'offerta o la promessa non sia accettata.

- Corruzione in atti giudiziari (art. 319 ter c.p.) – Tale ipotesi di reato si verifica qualora il dipendente o rappresentante della Società corrompa un magistrato o un testimone al fine di ottenere favori in un procedimento civile, penale o amministrativo che vede coinvolta la stessa Società o un soggetto terzo.
- Induzione indebita a dare o promettere utilità (art. 319 quater c.p.) – Tale ipotesi di reato si configura nel caso in cui il Pubblico Ufficiale o l'incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità.
- Truffa in danno dello Stato o di altro ente pubblico (art. 640 c.p.) – Tale ipotesi di reato si realizza qualora un dipendente o rappresentante della Società, attraverso artifici o raggiri, induca lo Stato o un Ente Pubblico in errore, ricavandone un profitto cagionando un danno allo Stato o all'ente pubblico.
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.) – Tale ipotesi di reato si realizza qualora un dipendente o rappresentante della Società, attraverso artifici o raggiri, induca lo Stato o un ente pubblico o Istituzioni Comunitarie in errore, ottenendo contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo.
- Frode informatica se commessa in danno dello Stato o di altro Ente Pubblico (art. 640 ter c.p.) – Tale ipotesi di reato si configura nel caso di alterazione del funzionamento di un sistema informatico o telematico o di intervento senza diritto su dati, informazioni, programmi allo scopo di trarne profitto con danno d'altri.
- Concussione, induzione indebita a dare o promettere utilità, 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.) – Tale ipotesi di reato si configura nel caso in cui un dipendente o rappresentante della Società commetta i delitti di corruzione e istigazione alla corruzione con riguardo ai membri delle istituzioni comunitarie.

- Malversazione ai danni dello Stato (art. 316 bis c.p.) – Tale reato si configura nel caso in cui la Società abbia ottenuto l'erogazione, da parte dello Stato o altro Ente Pubblico o dalle Comunità Europee, di contributi, sovvenzioni o finanziamenti destinati alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, ma non li abbia destinati a tali finalità.
- Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.) – Tale reato si configura nel caso in cui la Società abbia ottenuto contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, da parte dello Stato o altri Enti Pubblici o dalla Comunità Europea, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti il falso, oppure mediante l'omissione di informazioni dovute.
- Concussione (art. 317 c.p.) – Tale ipotesi di reato si configura nel caso in cui il Pubblico Ufficiale, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

Le attività a rischio reato nella PA si riferiscono a comportamenti posti in essere da amministratori, dirigenti e dipendenti della Società per le attività svolte nelle “aree a rischio”, nonché da Collaboratori Esterni.

Obiettivo del presente paragrafo è che tutti i Destinatari, come sopra individuati, adottino regole di condotta uniformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

Prevedendo l'espresso divieto – a carico degli Esponenti Aziendali in via diretta ed a carico dei Collaboratori Esterni tramite apposite clausole contrattuali – di:

- Porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto).

- Porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.
- Porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:

- Effettuare elargizioni in denaro a pubblici funzionari ovvero accettare elargizioni in denaro.
- Distribuire ovvero accettare omaggi e regali qualora gli stessi eccedano le normali pratiche commerciali o di cortesia ovvero siano rivolti ad acquisire o garantire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsivoglia vantaggio alla società. Gli omaggi consentiti si caratterizzano per l'esiguità del loro valore; i regali offerti devono essere documentati in modo adeguato per consentire le eventuali verifiche.
- Accordare altri vantaggi di qualsiasi natura (es.: promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione.
- Riconoscere compensi in favore dei Collaboratori Esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.
- Presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari ovvero accettare dichiarazioni palesemente non veritiere al fine di favorire l'elargizione di erogazioni pubbliche, contributi o finanziamenti agevolati.
- Destinare somme ricevute da organismi pubblici nazionali o comunitari per scopi diversi da quelli cui le medesime erano destinate.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- I rapporti nei confronti della P.A. per le suddette aree di attività a rischio vengono gestiti dai Responsabili interni interessati, i quali saranno tenuti ad informare l'Amministratore Unico della Società sull'attività svolta.
- Gli incarichi conferiti ai Collaboratori Esterni devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito e devono essere proposti o verificati o approvati dall'Amministratore Unico.
- Nessun corrispettivo dovrà essere pagato in contanti né tanto meno in natura.
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari devono contenere solo elementi assolutamente veritieri.
- Coloro che svolgono una funzione di supervisione e controllo su adempimenti connessi allo svolgimento delle suddette attività (es.: pagamento di fatture, destinazione di finanziamenti o altre erogazioni pubbliche) devono porre particolare attenzione nell'attuazione degli adempimenti stessi e riferire immediatamente all'ODV eventuali situazioni ritenute irregolari.

In sede di mappatura sono state identificate le seguenti attività a rischio di compimento di reati/illeciti amministrativi riconducibili a reati contro la Pubblica Amministrazione:

- FATTURAZIONE.
- ACCESSO ALLA RETE INFORMATICA AZIENDALE.
- RAPPORTI CON REGIONE E ALTRI ENTI PUBBLICI.
- ASSUNZIONE DI PERSONALE E CONFERIMENTO INCARICHI DI CONSULENZA.
- RAPPORTI CON I FORNITORI E CONFERIMENTO INCARICHI DI CONSULENZA.

Delle attività svolte nelle aree considerate "a rischio" è necessario garantire l'"evidenza". In ogni momento, dovrà essere possibile identificare i soggetti intervenuti nelle fasi che caratterizzano le operazioni e le modalità seguite per il perfezionamento del processo decisionale. La responsabilità dell'attività svolta nelle aree considerate "a rischio" è

assegnata, secondo competenza, ai Responsabili interni. L'“evidenza” potrà essere garantita anche per il tramite di idonee registrazioni informatiche.

I Responsabili individuati saranno tenuti:

- ad assicurare pronta informativa all'ODV relativamente alle nuove operazioni o tipologia di operazioni “a rischio” intraprese ovvero a nuove “aree a rischio” rispetto a quelle già individuate;
- a garantire all' ODV l'accessibilità a tutti i documenti riguardanti le singole operazioni effettuate nell'ambito delle aree di attività definite “a rischio”;
- ad informare l' ODV sulla chiusura delle singole operazioni “a rischio” ovvero sulla cessazione dell'attività in aree considerate “a rischio”;
- ad assicurare al personale la formazione ritenuta necessaria per una corretta operatività nell'ambito delle aree “a rischio” ed un adeguato livello informativo sui rischi ai quali la medesima è soggetta.
- Nei casi in cui dovessero intervenire, per il perfezionamento dell'operazione “a rischio”, Collaboratori Esterni, i Responsabili dovranno richiedere che venga rilasciata per iscritto una dichiarazione dalla quale dovrà risultare che gli stessi sono pienamente a conoscenza degli adempimenti da espletare e degli obblighi da osservare nello svolgimento dell'operazione e che si impegnano ad improntare i comportamenti finalizzati all'attuazione dell'iniziativa comune a principi di trasparenza e correttezza e nella più stretta osservanza delle disposizioni di Legge.

PRINCIPI SPECIFICI:

FATTURAZIONE

È vietato emettere fatture per prestazioni non realmente erogate o duplicare la fatturazione per una stessa prestazione. È vietato, altresì, non emettere note di credito laddove siano state fatturate, anche se per errore, prestazioni in tutto o in parte inesistenti.

ACCESSO ALLA RETE INFORMATICA

Ad ogni operatore autorizzato ad accedere alla rete informatica aziendale sono attribuite una user ID e una password personali, che lo stesso si impegna a non comunicare a terzi. È vietato utilizzare la user ID o la password di altro operatore.

RAPPORTI CON REGIONE E ALTRI ENTI PUBBLICI

L'Amministratore Unico di Techem S.r.l., o persona dallo stesso formalmente delegata, tiene i rapporti con le autorità e i funzionari regionali, comunali, provinciali e delle altre istituzioni pubbliche nazionali o comunitarie, ovvero con privati con i quali Techem S.r.l. venga in rapporto.

I soggetti ora menzionati, nell'ambito delle loro rispettive competenze, hanno analogo obbligo informativo nei confronti dell'ODV. È vietato a tutti i soggetti previsti dal Decreto offrire, promettere o consegnare denaro, doni o altra utilità, anche per interposta persona, a pubblici ufficiali o incaricati di pubblico servizio, anche delle Comunità europee, di ogni qualifica o livello, al loro coniuge ovvero ai loro ascendenti, discendenti, fratelli, sorelle o a persone da quelle indicate, salvo che il fatto si verifichi in occasione di festività in cui sia tradizione lo scambio di doni o, comunque, questi siano di tenue valore o si riferisca a contribuzioni, nei limiti consentiti dalla legge, in occasione di campagne elettorali.

Ogni spesa di rappresentanza deve essere prontamente rendicontata.

Eventuali locazioni o acquisti di immobili dalle pubbliche amministrazioni, con le quali la Società abbia stabilmente rapporti, devono essere attestate da apposita perizia di un esperto che attesti la corrispondenza del valore dei contratti con quelli di mercato.

ASSUNZIONE DEL PERSONALE E CONFERIMENTO INCARICHI DI CONSULENZA

È vietata alla società Techem S.r.l. l'assunzione di ex impiegati della pubblica amministrazione, anche delle Comunità europee, nei due anni successivi al compimento di un atto, di competenza di uno dei predetti soggetti ed espressione del suo potere

discrezionale, da cui sia derivato un vantaggio per la Società. Il divieto sussiste anche per le ipotesi di omissione o ritardo di un atto svantaggioso per la Società.

RAPPORTI CON I FORNITORI E CONFERIMENTO INCARICHI DI CONSULENZA

I fornitori devono essere selezionati in base a criteri di scelta individuati nel rispetto della legislazione regionale, nazionale e comunitaria e in base alla loro capacità di fornire prodotti o servizi rispondenti per qualità, costo e puntualità, all'esigenza di garantire l'efficacia della prestazione aziendale finale.

Gli incarichi di consulenza esterna devono essere conferiti solo in presenza di reali esigenze aziendali e la relativa proposta deve essere formalizzata per iscritto recando l'indicazione espressa del compenso pattuito.

I contratti stipulati con consulenti e fornitori devono contenere specifiche clausole per l'immediata risoluzione del rapporto nelle ipotesi di inosservanza del Modello, nonché di elusione fraudolenta dello stesso, limitatamente alle procedure attinenti all'oggetto dell'incarico o alla effettuazione della prestazione.

7.2 Reati di criminalità informatica

Tra i reati di criminalità informatica previsti dal Decreto si indicano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da Techem:

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società falsifichi un documento informatico pubblico o privato, avente efficacia probatoria. A tal fine, per “documento informatico” si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, con esclusione dunque dei programmi informatici.
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. A tal fine, per “sistema informatico” si intende qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati.
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici o parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo, al fine di procurare a sé o ad altri un profitto o di recare un danno ad altri.
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante

o un dipendente della Società si procuri, diffonda, comunichi o consegna un programma informatico avente per scopo o per effetto di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione (totale o parziale) o l'alterazione del suo funzionamento.

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) - Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società intercetti fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa. Il reato si configura altresì qualora si riveli, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle predette comunicazioni.
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) - Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società installi apparecchiature atte a intercettare, impedire, o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) - Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società distrugga, deteriori, cancelli, alteri o renda inservibili, anche parzialmente, informazioni, dati o programmi informatici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.
- 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.) - Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società distrugga, deteriori, cancelli o renda inservibili informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente Pubblico, o comunque di

pubblica utilità. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.

- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società distrugga, danneggi, deteriori, o renda inservibili, anche parzialmente, sistemi informatici o telematici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.) – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Società distrugga, danneggi, deteriori, renda inservibili, anche parzialmente, i sistemi informatici o telematici di pubblica utilità, ovvero ne ostacoli il corretto funzionamento. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.) – Tale ipotesi di reato si configura nel caso in cui il soggetto che presta servizi di certificazione di firma elettronica violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri un danno. Trattandosi di un reato proprio, lo stesso sarà configurabile per Techem qualora la condotta venga posta in essere in concorso con il soggetto “che presta servizi di certificazione delle firme elettroniche”.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori, dirigenti e dipendenti della Società, nonché da Collaboratori Esterni.

L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle “aree a rischio”, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati di criminalità informatica.

In particolare, il presente paragrafo ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'ODV, ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

In particolare, nell'espletamento delle attività considerate "a rischio", i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne.

AREE A RISCHIO

In sede di mappatura è stata identificata l'attività GESTIONE DATABASE a rischio di compimento di reati/illeciti amministrativi riconducibili a reati di criminalità informatica.

DISPOSIZIONI E PRINCIPI SPECIFICI

Si indicano qui di seguito le disposizioni ed i principi specifici che, in relazione ad ogni singola area a rischio devono essere rispettati da tutti i Destinatari ad integrazione delle altre procedure aziendali esistenti.

GESTIONE DATABASE

Techem S.r.l. verifica, tramite idonea documentazione, l'identità dei soggetti ai quali consente l'accesso ai propri database ovvero la veridicità dei dati identificanti i soggetti autorizzati all'accesso.

Techem S.r.l. custodisce copia della suddetta documentazione per l'intera durata di

validità delle credenziali di autenticazione concesse. L'autorizzazione all'accesso viene revocata contestualmente alla cessazione del rapporto contrattuale. E' fatto salvo il diritto del titolare dell'informazione di richiederne formalmente l'integrazione, la cancellazione, o la rettifica che dovranno avvenire tramite un apposito profilo, utilizzabile esclusivamente da un soggetto autorizzato per il tempo strettamente necessario al compimento di tale operazione.

Per nessuna ragione Techem S.r.l. consentirà che uno degli operatori di sistema abbia all'interno del suo abituale profilo la possibilità di effettuare le suddette modifiche.

È fatto divieto a tutto il personale dipendente, agli amministratori, e al personale:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al sistema informatico o telematico di Techem al fine di alterare e/o cancellare dati e/o informazioni;
- danneggiare informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità

7.3 Reati di criminalità organizzata

Tra i reati di criminalità organizzata previsti dal Decreto si indicano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da Techem:

- Associazione per delinquere (art. 416 c.p.). Il reato si configura qualora tre o più persone si associano allo scopo di commettere più delitti. Coloro che promuovono o costituiscono od organizzano l'associazione sono puniti con la reclusione da tre a sette anni; per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. I capi soggiacciono alla stessa pena stabilita per i promotori. La pena è aumentata se il numero degli associati è di dieci o più. Se l'associazione è diretta a commettere uno dei delitti di cui agli articoli 600 c.p. (riduzione o mantenimento in schiavitù o in servitù), 601 c.p. (tratta di persone) e 602 c.p. (acquisto e alienazione di schiavi), nonché all'articolo 12, comma 3-bis del Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero di cui al D.Lgs. n. 286/98 (disposizioni contro le immigrazioni clandestine), si applica la reclusione da cinque a quindici anni nei casi di promozione, costituzione, organizzazione dell'associazione e da quattro a nove anni nei casi di mera partecipazione all'associazione.
- Associazione per delinquere di tipo mafioso (art. 416 bis c.p.). Il reato si configura nei confronti di chiunque faccia parte di un'associazione di tipo mafioso formata da tre o più persone; il partecipante è punito con la reclusione da sette a dodici anni. Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da nove a quattordici anni. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici 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. Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene summenzionate sono aumentate da un terzo alla metà. Tali disposizioni si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

- Delitti commessi avvalendosi delle condizioni del predetto art. 416 bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo (art. 24 ter, primo comma, D.Lgs. 231/2001). Tale previsione normativa è volta a sanzionare i delitti commessi avvalendosi della forza intimidatrice del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva, nonché il reato di c.d. concorso esterno nell'associazione mafiosa, fattispecie di elaborazione giurisprudenziale, che si ravvisa nella condotta di un soggetto esterno all'associazione a delinquere che apporti un contributo causale determinante al perseguimento degli scopi illeciti e alla vita stessa dell'associazione mafiosa. I requisiti per la configurabilità del concorso esterno in associazione mafiosa sono i seguenti: l'occasionalità e l'autonomia del contributo prestato; la funzionalità del contributo al perseguimento degli scopi associativi e l'efficienza causale del contributo al rafforzamento e al consolidamento dell'associazione; inoltre è necessaria la sussistenza, in capo al soggetto agente del dolo, ossia la consapevolezza di favorire il conseguimento degli scopi illeciti. Ai sensi dell'art.7 legge l.12 luglio 1991 nr. 203, per i delitti punibili con pena diversa dall'ergastolo commessi avvalendosi delle condizioni previste dall'art. 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, la pena è aumentata da un terzo alla metà.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori, dirigenti e dipendenti della Società, nonché da Collaboratori Esterni.

L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle "aree a rischio", si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati di criminalità organizzata.

In particolare, il presente paragrafo ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'ODV, ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

In particolare, nell'espletamento delle attività considerate "a rischio", i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne.

AREE A RISCHIO

- GESTIONE DEI RAPPORTI CON L'AMMINISTRAZIONE FINANZIARIA;
- SELEZIONE, ASSUNZIONE E GESTIONE DELLE RISORSE UMANE;
- APPROVVIGIONAMENTO DI BENI E SERVIZI;
- ASSEGNAZIONE E GESTIONE DI INCARICHI DI CONSULENZA;
- GESTIONE AGENTI E PROCACCIATORI;
- NEGOZIAZIONE, STIPULAZIONE ED ESECUZIONE DI CONTRATTI E ACCORDI ATTIVI CON SOGGETTI PRIVATI;

PRINCIPI SPECIFICI:

GESTIONE DEI RAPPORTI CON L'AMMINISTRAZIONE FINANZIARIA

Si riferisce all'Area di gestione dei rapporti con l'Amministrazione Finanziaria in merito alle attività svolte dalla Società nell'ambito della gestione degli adempimenti e delle scadenze previste per il rispetto della normativa fiscale vigente. La Società si avvale della consulenza di uno Studio Esterno per il supporto in ambito fiscale.

I Consulenti Esterni devono essere selezionati in base a criteri di scelta individuati nel rispetto della legislazione vigente ed in base alla loro capacità di fornire un servizio rispondenti per qualità, costo e puntualità, all'esigenza di garantire l'efficacia della prestazione aziendale finale. I contratti stipulati con i Consulenti devono contenere specifiche clausole per l'immediata risoluzione del rapporto nelle ipotesi di inosservanza del Modello, nonché di elusione fraudolenta dello stesso, limitatamente alle procedure attinenti all'oggetto dell'incarico o alla effettuazione della prestazione.

È vietato emettere fatture per prestazioni non realmente erogate o duplicare la fatturazione per una stessa prestazione. È vietato, altresì, non emettere note di credito laddove siano state fatturate, anche se per errore, prestazioni in tutto o in parte inesistenti.

È obbligatorio tenere le scritture contabili in regola con la normativa vigente in materia. È obbligo della Società nominare un Responsabile d'Area che relazionerà sul suo operato all'Amministratore Unico ed all'ODV sul rispetto del presente Modello e del Codice Etico e di tutte le procedure aziendali ad essi connesse.

SELEZIONE, ASSUNZIONE E GESTIONE DELLE RISORSE UMANE

L'Area si riferisce alla gestione delle attività inerenti all'inserimento nell'organizzazione aziendale di risorse umane: dalla segnalazione del fabbisogno, alla selezione del candidato, fino alla definizione della modalità di inserimento (inquadramento e livello retributivo). La gestione delle attività di selezione del Personale può essere sia interna sia supportata da agenzie interinali. All'avvio di un processo di selezione, sia esso gestito direttamente o tramite agenzie, il Responsabile Direzione Personale e Affari Generali provvede a individuare i contenuti del Job Profile, quindi predispone e diffonde l'annuncio di lavoro. In seguito ad un'analisi dei curricula dei candidati, un Addetto della Direzione Personale e Affari Generali effettua un primo colloquio. Si prosegue, quindi, ad un secondo colloquio "tecnico" con il Capo Ufficio che ha richiesto la risorsa da inserire in azienda. Se il candidato supera entrambi i colloqui è previsto l'inserimento in Azienda per un periodo di prova a conclusione del quale le Funzioni coinvolte decidono in merito all'inserimento in azienda.

APPROVVIGIONAMENTO DI BENI E SERVIZI

L'Area si riferisce alle attività di approvvigionamento di beni e servizi riconducibili alle seguenti categorie:

- Materie prime;
- Materie sussidiarie;
- Servizi per lavorazioni esterne;
- Beni strumentali;
- Servizi generali (pulizia, etc);
- Trasporti;
- Servizi relativi ai sistemi informatici.

La selezione e qualifica di un Fornitore prevede l'acquisizione di informazioni sul potenziale fornitore che permettano di stabilirne il grado di affidabilità e di aderenza ai requisiti attesi. Gli elementi di valutazione preventiva sono riconducibili a notizie sulla struttura organizzativa e referenze (esempio, altre aziende fornite nel settore), caratteristiche proprie della fornitura. L'Ufficio Amministrazione riceve le fatture ed effettua una verifica di conformità rispetto all'ordine di acquisto inserito a sistema.

Nel caso dovessero verificarsi anomalie rispetto agli importi fatturati, viene informato il Responsabile d'Area interessato dalla funzione che provvederà ad effettuare i dovuti controlli.

ASSEGNAZIONE E GESTIONE DI INCARICHI DI CONSULENZA

L'Area riguarda le attività svolte nell'ambito dell'assegnazione e gestione di incarichi di consulenza esterna.

I servizi di consulenza di cui si avvale la Società possono essere classificati nelle seguenti tipologie:

- legali amministrative e fiscali;
- tecniche e commerciali.

Con riferimento alle modalità di qualifica e selezione dei consulenti, si rimanda a quanto descritto per l'Area approvvigionamento di beni e servizi. L'Ufficio Amministrazione che riceve le fatture deve effettuare una verifica di conformità rispetto al servizio richiesto ed alle condizioni contrattuali del Consulente.

GESTIONE AGENTI E PROCACCIATORI

L'Area descrive le attività inerenti la gestione dei rapporti con Agenti e Procacciatori. Per la gestione delle vendite Techem si avvale di diversi Agenti e Procacciatori organizzati per mercato di riferimenti. Gli agenti operano in diverse aree geografiche dell'Italia. La ricerca e la selezione di nuovi Agenti è curata dalla Società con una selezione che tenga in considerazione oltre alle capacità commerciali e relazionali, della conoscenza del settore e dell'esperienza pluriennale nel campo, anche dei principi di cui al presente Modello ed al Codice Etico.

Techem si avvale di Agenti e Procacciatori con i quali ha rapporti consolidati da molti anni ed il turnover è molto limitato.

Per la fatturazione ed il pagamento si rimanda a quanto in precedenza definito per l'Area assegnazione e gestione di incarichi di consulenza.

NEGOZIAZIONE, STIPULAZIONE ED ESECUZIONE DI CONTRATTI E ACCORDI ATTIVI CON SOGGETTI PRIVATI

L'Area si riferisce alla negoziazione/stipulazione/esecuzione dei contratti con i clienti privati. La ricerca e l'individuazione di nuovi clienti può avvenire sia tramite la Direzione Commerciale che tramite gli Agenti o Procacciatori. In fase di offerta, i prezzi e le condizioni commerciali di vendita sono definite sulla base delle indicazioni della Direzione Commerciale. La conferma d'ordine viene fornita attraverso l'emissione di un ordine formale da parte del cliente oppure attraverso la firma per accettazione del preventivo presentato da Techem.

I Destinatari coinvolti in tale Processo devono:

- assicurare che i contratti con i clienti siano chiari, completi, dettagliati e conclusi in coerenza con le politiche commerciali definite dalla Società;
- assicurare un sistematico aggiornamento degli standard contrattuali coerentemente con le evoluzioni della normativa vigente;

- assicurare che gli accordi con i terzi siano formalizzati mediante redazione di un contratto/lettera d'incarico, debitamente autorizzato da soggetti muniti di idonei poteri e che riportino indicazione del compenso pattuito, del dettaglio della eventuale prestazione di servizi da effettuare;
- assicurare l'inserimento di clausole contenenti l'impegno del cliente di comunicare senza indugio eventuali contestazioni proveniente da terzi circa la titolarità di diritti di proprietà industriale o segni distintivi, o contestazioni sulle caratteristiche dei beni o sui segni distintivi dei beni;
- assicurare l'inserimento di clausole nei contratti con gli agenti che prevedano l'impegno al rispetto di regole di correttezza commerciale idonee a prevenire condotte fraudolente in danno dei clienti;
- assicurare che ogni accordo con i clienti terzi coinvolti in tale Area Sensibile contenga apposita clausola relativa al D.Lgs. 231/01 che preveda la risoluzione del contratto in relazione ad eventuali inadempienze dei principi contenuti nel Codice Etico e nel Modello di organizzazione, gestione e controllo aziendale;
- assicurare, in ogni fase del processo relativo all'Area Sensibile in esame, il rigoroso rispetto delle regole di correttezza commerciale dettate dalla Società ed il rispetto delle leggi e regolamenti a tutela del mercato, del consumatore e del cliente finale in genere, in ossequio ai principi di trasparenza, completezza informativa, buona fede e chiarezza.

7.4 Reati contro l'industria e il commercio

Tra i reati contro l'industria e il commercio previsti dal Decreto si indicano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da Techem:

- Frode nell'esercizio del commercio (art. 515 c.p.) – Tale reato si configura qualora taluno, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita. Tale ipotesi è punita, qualora il fatto non costituisca un più grave delitto, con la reclusione fino a due anni o con la multa fino a Euro 2.065. Se si tratta di oggetti preziosi, la pena è della reclusione fino a tre anni o della multa non inferiore a Euro 103.
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.) – Tale reato si configura qualora taluno ponga in vendita o metta altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto. Tale ipotesi è punita, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a due anni e con la multa fino a 20.000 Euro.
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriali (art. 517-ter c.p.) – Salva l'applicazione degli artt. 473 e 474 c.p., tale reato si configura qualora taluno, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso. Tale reato è punito, a querela della persona offesa, con la reclusione fino a due anni e con la multa fino a Euro 20.000. Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al

primo comma. In questi casi, i delitti sono punibili sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale;

- Turbata libertà dell'industria e del commercio (art. 513 c.p.) Il reato si configura qualora taluno adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio. Tale ipotesi è punita, a querela della persona offesa, se il fatto non costituisce un più grave reato, con la reclusione fino a due anni e con la multa da Euro 103 a Euro 1.032;
- Illecita concorrenza con minaccia o violenza (art. 513 bis c.p.) Il reato si configura qualora taluno, nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compia atti di concorrenza con violenza o minaccia. Tale ipotesi è punita con la reclusione da due a sei anni. La pena è aumentata se gli atti di concorrenza riguardano un'attività finanziata in tutto o in parte ed in qualsiasi modo dallo Stato o da altri enti pubblici.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

Le Aree identificate come a rischio di commissione dei Reati ai sensi del Decreto sono emersi dall'analisi di risk assessment.

Con riferimento specifico ai reati contro l'industria e il commercio, ai fini della presente Parte Speciale, i Processi Sensibili sono stati circoscritti ai seguenti:

- APPROVVIGIONAMENTO DI BENI DESTINATI ALLA LAVORAZIONE E SERVIZI
- NEGOZIAZIONE, STIPULAZIONE E ESECUZIONE DI CONTRATTI E ACCORDI CON SOGGETTI PRIVATI

Eventuali integrazioni delle suddette Aree Sensibili a rischio potranno essere richieste a cura dell'Organismo di Vigilanza della Società, al quale viene dato mandato di identificare le relative ipotesi e di definire gli opportuni provvedimenti operativi affinché la Società provveda a modificare e/o integrare conseguentemente il Modello.

PRINCIPI SPECIFICI

APPROVVIGIONAMENTO DI BENI DESTINATI ALLA LAVORAZIONE E SERVIZI

L'Area si riferisce alle attività di approvvigionamento di beni e servizi riconducibili alle seguenti categorie:

- Materie prime;
- Materie sussidiarie;
- Servizi per lavorazioni esterne;
- Beni strumentali;
- Servizi generali (pulizia, etc);
- Trasporti;
- Servizi relativi ai sistemi informatici.

La selezione e qualifica di un Fornitore prevede l'acquisizione di informazioni sul potenziale fornitore che permettano di stabilirne il grado di affidabilità e di aderenza ai requisiti attesi. Gli elementi di valutazione preventiva sono riconducibili a notizie sulla struttura organizzativa e referenze (esempio, altre aziende fornite nel settore), caratteristiche proprie della fornitura. L'Ufficio Amministrazione riceve le fatture ed effettua una verifica di conformità rispetto all'ordine di acquisto inserito a sistema.

Nel caso dovessero verificarsi anomalie rispetto agli importi fatturati, viene informato il Responsabile d'Area interessato dalla funzione che provvederà ad effettuare i dovuti controlli.

NEGOZIAZIONE, STIPULAZIONE E ESECUZIONE DI CONTRATTI E ACCORDI CON SOGGETTI PRIVATI

L'Area si riferisce alla negoziazione/stipulazione/esecuzione dei contratti con i clienti privati.

La Techem s.r.l. è una società di proprietà della Techem Energy services G.M.B.H. con sede in Germania . La casa madre fornisce alla Techem s.r.l. quasi tutti i prodotti (70%), le

infrastrutture (call service, formazione, software e relativa assistenza). La Techem s.r.l. nasce nel 1995 ed è leader mondiale nel mercato delle apparecchiature di rilevamento radio installate. La casa madre è sul mercato da più di 55 anni ed è stata la prima società a:

- sviluppare la tecnologia relativa alla ripartizione di calore per sistemi di riscaldamento centralizzato nei condomini.
- Introdurre un modulo di regolazione ad onde-radio “enotech” che gestisce il flusso di calore prodotto dalla caldaia termica in funzione della quantità di calore richiesto dal singolo calorifero. I dati vengono trasmessi regolarmente ad “enotech” dal singolo ripartitore di calore Techem.

L'attività direzionale e produttiva è svolta nella sede centrale, nelle filiali viene effettuato il processo produttivo.

L'obiettivo della Techem S.r.l. è quello di effettuare servizi fedeli alle aspettative dei clienti ed entro i tempi stabiliti dai contratti.

La ricerca e l'individuazione di nuovi clienti può avvenire sia tramite la Direzione Commerciale che tramite gli Agenti o Procacciatori. In fase di offerta, i prezzi e le condizioni commerciali di vendita sono definite sulla base delle indicazioni della Direzione Commerciale. La conferma d'ordine viene fornita attraverso l'emissione di un ordine formale da parte del cliente oppure attraverso la firma per accettazione del preventivo presentato da Techem.

I Destinatari coinvolti in tale Processo devono:

- assicurare che i contratti con i clienti siano chiari, completi, dettagliati e conclusi in coerenza con le politiche commerciali definite dalla Società;
- assicurare un sistematico aggiornamento degli standard contrattuali coerentemente con le evoluzioni della normativa vigente;
- assicurare che gli accordi con i terzi siano formalizzati mediante redazione di un contratto/lettera d'incarico, debitamente autorizzato da soggetti muniti di idonei poteri e che riportino indicazione del compenso pattuito, del dettaglio della eventuale prestazione di servizi da effettuare;

- assicurare l'inserimento di clausole contenenti l'impegno del cliente di comunicare senza indugio eventuali contestazioni proveniente da terzi circa la titolarità di diritti di proprietà industriale o segni distintivi, o contestazioni sulle caratteristiche dei beni o sui segni distintivi dei beni;
- assicurare l'inserimento di clausole nei contratti con gli agenti che prevedano l'impegno al rispetto di regole di correttezza commerciale idonee a prevenire condotte fraudolente in danno dei clienti;
- assicurare che ogni accordo con i clienti terzi coinvolti in tale Area Sensibile contenga apposita clausola relativa al D.Lgs. 231/01 che preveda la risoluzione del contratto in relazione ad eventuali inadempienze dei principi contenuti nel Codice Etico e nel Modello di organizzazione, gestione e controllo aziendale;
- assicurare, in ogni fase del processo relativo all'Area Sensibile in esame, il rigoroso rispetto delle regole di correttezza commerciale dettate dalla Società ed il rispetto delle leggi e regolamenti a tutela del mercato, del consumatore e del cliente finale in genere, in ossequio ai principi di trasparenza, completezza informativa, buona fede e chiarezza.

7.5 Reati societari

Il Decreto prevede una serie di reati societari, tra i quali si ritiene che quelli che possono essere commessi nell'ambito dell'attività svolta da Techem siano i seguenti:

- False comunicazioni sociali (art. 2621 c.c.) – Tale ipotesi di reato si realizza se gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci, i liquidatori della Società, con l'intenzione di ingannare i soci o il pubblico e al fine di trarre ingiusto profitto, espongono nei bilanci, relazioni o altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ovvero omette di fornire notizie la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società o del Gruppo di appartenenza, in modo idoneo a indurre in errore i destinatari delle suddette comunicazioni.
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.) – Tale fattispecie di reato sussiste, qualora ricorrano gli elementi richiesti per il realizzarsi del precedente illecito e vi sia un danno patrimoniale per i soci o per i creditori.
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.) – Tale figura di reato si realizza qualora il revisore della Società, al fine di conseguire un ingiusto profitto per la Società, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e con l'intenzione di ingannare i destinatari delle comunicazioni, attesti il falso od occulti informazioni concernenti la situazione economica, patrimoniale o finanziaria della Società, in modo idoneo ad indurre in errore i destinatari di dette comunicazioni.
- Impedito controllo (art. 2625, 2° comma c.c.) – Tale reato si configura qualora, occultando documenti o con altri idonei artifici, gli amministratori di TECEM impediscano o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, al collegio sindacale o alla società di revisione cagionando un danno ai soci.

- Indebita restituzione dei conferimenti (art. 2626 c.c.) – Tale figura di reato si realizza nel caso in cui un amministratore della Società, fuori dei casi di legittima riduzione del capitale sociale e sotto qualsiasi forma, restituisca ai soci i conferimenti o li liberi dall'obbligo di eseguirli.
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.) – Tale figura di reato ricorre nel caso in cui gli amministratori della Società ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite.
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.) – Tale figura di reato si configura qualora gli amministratori della Società acquistino o sottoscrivano, al di fuori dei casi previsti dalla legge, azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.) – Tale figura di reato si realizza nel caso in cui gli amministratori della Società, violando le disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.
- Formazione fittizia del capitale (art. 2632 c.c.) – Tale figura di reato si configura qualora gli amministratori e i soci conferenti della Società, anche in parte, formino od aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o di quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della Società nel caso di trasformazione.
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.) – Tale fattispecie di reato si configura nell'ipotesi in cui l'eventuale liquidatore della Società, ripartendo i beni sociali prima del pagamento dei creditori sociali o

dell'accantonamento delle somme necessarie per soddisfarli, cagioni danno ai creditori stessi.

- Corruzione tra privati (art. 2635 c.c.) - Tale fattispecie di reato si può configurare qualora un esponente della Società dia o prometta denaro o altra utilità ad un esponente di un'altra società (amministratore, direttore generale, dirigente preposto alla redazione dei documenti contabili societari, sindaco, liquidatore o soggetti sottoposti alla direzione e vigilanza dei primi), affinché questo compia od ometta atti, in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà, cagionando nocumento a tale società.
- Illecita influenza sull'assemblea (art. 2636 c.c.) - Tale fattispecie di reato si configura nell'ipotesi in cui un soggetto apicale della Società o un sottoposto alla direzione e vigilanza di uno di questi (il reato può, infatti, essere commesso da "chiunque", quindi anche da soggetti esterni alla Società), con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.
- Aggiotaggio (art 2637 c.c.) - Tale fattispecie di reato ricorre qualora, ad esempio, il soggetto apicale di Techem diffonda notizie false ovvero ponga in essere operazioni simulate o altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art 2638 c.c.) - Tale fattispecie di reato si realizza qualora nelle comunicazioni alle autorità di vigilanza previste ai sensi della normativa applicabile in materia si espongano fatti materiali non corrispondenti al vero, ovvero si occultino con altri mezzi fraudolenti fatti che si sarebbero dovuti comunicare, al fine di ostacolare l'esercizio delle funzioni di vigilanza.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori, sindaci, liquidatori, dirigenti e dipendenti della Società, nonché da Collaboratori Esterni. L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle "aree a rischio", si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati Societari.

In particolare, il presente paragrafo ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

In particolare, nell'espletamento delle attività considerate "a rischio", i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati Societari;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera ed appropriata sulla situazione economica, patrimoniale e finanziaria della società.

In ordine a tale punto, è fatto divieto di:

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della società;
- omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della società.

AREE A RISCHIO

In relazione ai reati ed alle condotte criminose sopra esplicitate, le aree ritenute più specificatamente a rischio risultano essere le seguenti:

- la predisposizione di comunicazioni dirette ai soci ovvero al pubblico in generale riguardo alla situazione economica, patrimoniale e finanziaria della società (bilancio d'esercizio, relazioni semestrali, ecc.);
- la predisposizione e divulgazione verso l'esterno di dati o notizie relativi alla società.

In sede di mappatura sono state identificate le seguenti attività a rischio di compimento di reati/illeciti amministrativi riconducibili a reati societari e sono le seguenti:

- SOCIETARIA
- REDAZIONE DEI DOCUMENTI CONTABILI
- RAPPORTI CON GLI ORGANI DI CONTROLLO E LE AUTORITÀ DI VIGILANZA
- DISPOSIZIONE DEL PATRIMONIO SOCIALE
- DELIBERAZIONI ASSEMBLEARI

DISPOSIZIONI E PRINCIPI SPECIFICI

Si indicano qui di seguito le disposizioni ed i principi specifici che, in relazione ad ogni singola area a rischio devono essere rispettati da tutti i Destinatari ad integrazione delle altre procedure aziendali esistenti.

Nelle attività di predisposizione delle comunicazioni indirizzate ai soci ed al pubblico in generale e, in particolare, ai fini della formazione del bilancio, della relazione semestrale e di altre comunicazioni ufficiali, dovrà essere sempre sotto controllo la tempistica concernente la predisposizione delle comunicazioni medesime e dovranno essere assicurati:

- la veridicità, correttezza, precisione e completezza dei dati e delle informazioni;
- l'insussistenza di elementi da cui poter desumere che le dichiarazioni e i dati raccolti contengano elementi incompleti o inesatti.

Con riferimento all'attività di redazione del bilancio e di eventuali altri documenti informativi contabili, dovrà essere assicurato lo svolgimento di un'adeguata attività formativa ed informativa rivolta al personale dipendente (ed in particolare ai neo assunti) ed avente ad oggetto le principali nozioni e problematiche concernenti la redazione dei documenti contabili.

SOCIETARIA

Ai fini della salvaguardia degli interessi sociali, dei soci e dei creditori, gli organi sociali ed ogni altro soggetto coinvolto, anche di fatto, nell'attività societaria, devono osservare le disposizioni di legge a tutela dell'informazione e trasparenza societaria, nonché della formazione del capitale e della sua integrità.

REDAZIONE DEI DOCUMENTI CONTABILI

Il bilancio deve essere redatto con chiarezza e deve rappresentare in modo veritiero e corretto la situazione patrimoniale e finanziaria della società e il risultato economico dell'esercizio. I soggetti preposti alla formazione del bilancio, e altri prospetti contabili, devono uniformare le procedure contabili e amministrative ai principi contabili stabiliti dalla legge e dai regolamenti.

L'ODV può chiedere di esaminare la bozza di bilancio e la relativa nota integrativa in prossimità della approvazione del bilancio e chiedere chiarimenti ai responsabili della bozza di bilancio.

RAPPORTI CON GLI ORGANI DI CONTROLLO E LE AUTORITÀ DI VIGILANZA

L'Amministratore deve garantire il corretto svolgimento dell'attività di controllo agli organi e soggetti interni preposti a tali funzioni, anche soddisfacendo eventuali richieste di informazioni e rendendo loro disponibili i documenti necessari all'esercizio del controllo.

Nei rapporti con le Autorità pubbliche di vigilanza è fatto obbligo di effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste in base alla legge, e di non frapporre alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

DISPOSIZIONE DEL PATRIMONIO SOCIALE

Gli organi sociali devono osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale.

Ogni operazione idonea a incidere sull'integrità del patrimonio della società non può essere effettuata se non previa puntuale verifica in ordine alla consistenza dello stato patrimoniale.

Delle operazioni di cui al comma precedente deve essere data comunicazione all'ODV.

DELIBERAZIONI ASSEMBLEARI

Agli amministratori, agli organi di controllo, nonché a chiunque, a qualunque titolo, partecipi o assista all'Assemblea dei soci, è vietato compiere atti simulati o comportamenti fraudolentemente volti ad eludere le disposizioni civilistiche che regolano l'esercizio del diritto di voto, al fine di alterare il corretto procedimento di formazione della volontà assembleare e/o maggioranza richiesta per l'approvazione delle delibere.

7.6 Reati in tema di salute e sicurezza sul lavoro

I reati in materia di salute e sicurezza sul lavoro previsti dal Decreto che sono configurabili nell'ambito delle attività svolte da Techem sono i seguenti:

- Omicidio colposo (art. 589 c.p.). L'art. 25 septies, primo comma, del Decreto introduce, quale reato sanzionato ai sensi del Decreto stesso, il delitto di omicidio colposo commesso con violazione dell'articolo 55, comma 25, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, ovvero del D.Lgs. n. 81/2008. L'art. 25 septies, secondo comma, sanziona altresì il delitto di omicidio colposo di cui all'art. 589 del Codice Penale qualora esso sia commesso, in generale, con violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Ai sensi dell'art. 589 del Codice Penale, commette tale fattispecie di reato "chiunque cagiona per colpa la morte di una persona"; ai sensi del terzo comma del detto articolo, costituisce circostanza aggravante l'aver commesso il fatto con violazione delle "norme per la prevenzione degli infortuni sul lavoro". Tale ipotesi di reato potrebbe configurarsi nel caso in cui la violazione colposa delle norme sulla tutela della sicurezza e salute sul lavoro, adottate in azienda, determini un incidente sul lavoro che cagioni la morte di un dipendente della Società. Ad esempio, in ipotesi di morte a seguito di un incendio divampato nei locali aziendali a causa di un cortocircuito di un macchinario difettoso, in relazione al quale era stata negligenzemente omessa, da parte dei soggetti aziendali a ciò preposti, la periodica verifica di funzionalità e sicurezza.
- Lesioni personali colpose gravi e gravissime (art. 590 c.p.) L'art. 25 septies introduce altresì, quale reato sanzionato dal Decreto, il delitto di lesioni personali colpose di cui all'articolo 590, terzo comma, del Codice Penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Ai sensi dell'art. 590 del Codice Penale, commette tale fattispecie di reato "chiunque cagiona ad altri, per colpa, una lesione personale"; costituisce circostanza

aggravante, ai sensi del terzo comma del detto articolo, il fatto di aver cagionato la lesione personale con violazione delle “norme per la prevenzione degli infortuni sul lavoro”. Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

Tale ipotesi di reato potrebbe configurarsi nel caso in cui la violazione colposa delle norme sulla tutela della sicurezza e salute sul lavoro determini un incidente sul lavoro che cagioni a un dipendente della Società una lesione personale grave ovvero gravissima.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

La società Techem S.r.l. – in qualità di soggetto tenuto al rispetto del generale obbligo di tutela degli ambienti di lavoro sancito dall’art. 2087 c.c. – ha puntualmente e costantemente adempiuto nel tempo a quanto previsto dal complesso della legislazione in materia di sicurezza ed igiene sui luoghi di lavoro.

La prevenzione degli infortuni e la tutela della sicurezza e della salute sul luogo di lavoro rappresentano un’esigenza di fondamentale rilievo per la Società a protezione delle proprie risorse umane e dei terzi.

In tale contesto, la Società si impegna altresì a prevenire e reprimere comportamenti e pratiche che possano avere come effetto la mortificazione del dipendente nelle sue capacità e aspettative professionali, ovvero che ne determinino l’emarginazione nell’ambiente di lavoro, il discredito o la lesione della sua immagine.

Il sistema preventivo in esame è finalizzato a definire i compiti organizzativi e operativi e le responsabilità della direzione aziendale, dei dirigenti, dei preposti e dei lavoratori con specifico riguardo alle attività di sicurezza di rispettiva competenza.

AREE A RISCHIO

L'adozione e l'attuazione efficace del Modello Organizzativo ex D.lgs 231/01 necessita di un'attività di valutazione dei rischi preliminare finalizzata ad individuare, attraverso l'inventariazione e la mappatura delle aree e attività aziendali, i rischi di commissione dei reati previsti dal decreto ed a valutare il sistema di controllo interno e la sua capacità di mitigare i rischi identificati. Con riferimento ai reati in violazione delle norme in materia di sicurezza e salute sul lavoro, le stesse linee guida evidenziano l'impossibilità di escludere aprioristicamente alcun ambito di attività, poiché tali reati potrebbero interessare tutte le componenti aziendali. Inoltre per quanto concerne l'individuazione ed analisi dei rischi potenziali, nonché le possibili modalità attuative dei reati, sulla base delle già citate Linee Guida ed in ragione della già evidenziata natura integrata dell'organizzazione interna per la gestione della sicurezza e della salute sul lavoro in essere presso la società, l'analisi coincide con la valutazione dei rischi lavorativi effettuata dall'azienda in base alla legislazione prevenzionistica in vigore.

7.7 Reati di ricettazione, riciclaggio ed impiego di denaro, beni ed utilità di provenienza illecita

Si indicano di seguito le fattispecie di reato astrattamente configurabili nell'ambito delle attività svolte da Techem:

- Ricettazione (art. 648 c.p.) – Tale ipotesi di reato si configura nel caso in cui taluno acquisti o riceva o occulti denaro o cose provenienti da un qualsiasi delitto al fine di procurare a sé o ad altri un profitto. Ad esempio qualora il dirigente TECHEM incaricato di selezionare i fornitori e acquistare materie prime per la Società, acquisti una materia prima sotto costo perché proveniente da un illecito (ad es. furto), con profitto per la Società.
- Riciclaggio (art. 648 bis c.p.) – Tale ipotesi di reato si configura nel caso in cui taluno sostituisca o trasferisca denaro o beni provenienti da delitto non colposo ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare la loro provenienza delittuosa; ad esempio qualora l'Organo apicale di Techem incaricato degli acquisti per la società, versi quale corrispettivo ad un fornitore somme di denaro che sa provenire da un delitto, al fine di occultare tale provenienza.
- Impiego di denaro, beni o utilità di provenienza illecita (648-ter c.p.) – Tale ipotesi di reato si configura nel caso in cui taluno impieghi in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto; ad esempio qualora un Organo apicale Techem acquisti per la società un macchinario che sa provenire da un delitto (es. furto) utilizzandolo quale cespite aziendale e quindi nell'attività economica della società.

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori, e dipendenti della Società, nonché da Collaboratori Esterni.

L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle "aree a rischio", si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

In particolare, il presente paragrafo ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'ODV, ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

In particolare, nell'espletamento delle attività considerate "a rischio", i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne.

AREE A RISCHIO

In sede di mappatura sono state identificate le seguenti attività a rischio di compimento di reati/illeciti amministrativi riconducibili ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e sono le seguenti:

- ATTIVITÀ DI TESORERIA
- RAPPORTI COMMERCIALI

DISPOSIZIONI E PRINCIPI SPECIFICI

Si indicano qui di seguito le disposizioni ed i principi specifici che, in relazione ad ogni singola area a rischio devono essere rispettati da tutti i Destinatari ad integrazione delle altre procedure aziendali esistenti.

ATTIVITÀ DI TESORERIA

Le operazioni di trasferimento di denaro contante, di assegni di conto corrente, di vaglia postali, di assegni circolari, devono avvenire nel rispetto dei limiti previsti dalla normativa vigente in materia.

È vietata la sostituzione e il trasferimento di beni o denaro effettuati allo scopo di occultare o dissimulare l'origine illecita dei beni o del denaro, quando si abbia fondato motivo per ritenere che provengano da attività delittuosa. È altresì vietato, negli stessi casi, l'acquisto, la ricezione o l'occultamento di denaro o beni ovvero la dissimulazione della reale natura, provenienza, proprietà dei beni stessi.

Techem S.r.l. deve assicurare che il personale addetto al servizio di tesoreria riceva una adeguata informazione circa la tipologia di operazioni da considerare a rischio riciclaggio.

RAPPORTI COMMERCIALI

Si fa obbligo di procedere ad un'adeguata identificazione dei fornitori e ad una corretta conservazione della relativa documentazione. Tale procedura comporta, in particolare, l'acquisizione preventiva di informazioni commerciali sul fornitore, la valutazione del prezzo offerto in relazione a quello di mercato, l'effettuazione dei pagamenti ai soggetti che siano effettivamente controparti della transazione commerciale. Il sistema di acquisizione dati e la gestione degli stessi deve avvenire nel rispetto della normativa in materia di protezione dei dati personali.

7.8 Reati in violazione del diritto d'autore

Tra i reati in violazione del diritto d'autore previsti dal Decreto si indicano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da Techem:

- Art. 171, comma 1, lettera a-bis) e comma 3 della Legge del 22 aprile 1941 n. 633.
Il reato si configura qualora taluno, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa. In tal caso, la pena è una multa da Euro 51 a Euro 2.065, ma, secondo le disposizioni di cui al comma 3, la pena è della reclusione fino ad un anno o della multa non inferiore a Euro 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.
- Art. 171 bis della Legge del 22 aprile 1941 n. 633. Tale fattispecie è rivolta alla tutela del software (comma 1) e delle banche dati (comma 2). In particolare, il primo comma considera quale oggetto materiale della fattispecie i programmi per elaboratore ed i programmi contenuti in supporti non contrassegnati dalla SIAE, mentre le condotte tipizzate consistono nella abusiva duplicazione dei primi ovvero nella distribuzione, vendita, detenzione a scopo commerciale od imprenditoriale, concessione in locazione dei secondi, nonché in relazione a vicende volte unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. Il comma secondo, invece, contempla le condotte di riproduzione su supporti non contrassegnati SIAE, trasferimento su altro supporto, distribuzione, comunicazione, presentazione ovvero dimostrazione in pubblico del contenuto di una banca dati in violazione delle disposizioni di cui agli artt. 64 quinquies e 64 sexies della medesima Legge n. 633/1941, nonché di estrazione o reimpiego di banche dati in

violazione degli artt. 102 bis e 102 ter della stessa Legge n. 633/1941 ovvero, infine, di distribuzione, vendita, locazione di banche dati (sempre, evidentemente, prive del previsto contrassegno SIAE). Entrambe le disposizioni prevedono che tali condotte siano sorrette dal fine di profitto, delineando un sensibile ampliamento del contenuto dell'elemento soggettivo rispetto a quanto stabilito in passato laddove era invece richiesto il fine di lucro (che risulta invece richiesto per l'integrazione delle fattispecie di cui al successivo art. 171 ter), il quale, a differenza del fine di profitto, costituisce elemento di contenuto più limitato in quanto integrato solo in presenza di un "fine di guadagno economicamente apprezzabile o di incremento patrimoniale, a cui resta estraneo il mero risparmio di spesa al di fuori dello svolgimento di un'attività economica, e che non può identificarsi con un qualsiasi vantaggio di altro genere" (così Cass. pen., sez. III, 22.11.2006, Rizzi in CP, 2007, p. 2977).

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori, e dipendenti della Società, nonché da Collaboratori Esterni.

L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle "aree a rischio", si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati in violazione del diritto d'autore.

In particolare, il presente paragrafo ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'ODV, ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

In particolare, nell'espletamento delle attività considerate "a rischio", i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati in violazione del diritto d'autore;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne.

AREE A RISCHIO

In sede di mappatura è stata identificata la seguente attività a rischio di compimento di reati/illeciti amministrativi riconducibili ai reati in violazione del diritto d'autore illecita:

- GESTIONE SISTEMI INFORMATICI

DISPOSIZIONI E PRINCIPI SPECIFICI

Si indicano qui di seguito le disposizioni ed i principi specifici che, in relazione all'area a rischio devono essere rispettati da tutti i Destinatari ad integrazione delle altre procedure aziendali esistenti.

GESTIONE SISTEMI INFORMATICI

Questa Area si riferisce alla gestione dei sistemi informatici nel loro complesso con particolare riferimento a:

- attività di archiviazione e conservazione di documenti tutelati;
- utilizzo software tutelati da diritto d'autore.

Techem S.r.l. verifica, tramite idonea documentazione, l'identità dei soggetti ai quali consente l'accesso ai propri database ovvero la veridicità dei dati identificanti i soggetti autorizzati all'accesso.

Techem S.r.l. custodisce copia della suddetta documentazione per l'intera durata di validità delle credenziali di autenticazione concesse. L'autorizzazione all'accesso viene revocata contestualmente alla cessazione del rapporto contrattuale. E' fatto salvo il diritto del titolare dell'informazione di richiederne formalmente l'integrazione, la cancellazione, o la rettifica che dovranno avvenire tramite un apposito profilo, utilizzabile esclusivamente da un soggetto autorizzato per il tempo strettamente necessario al compimento di tale operazione.

Per nessuna ragione Techem S.r.l. consentirà che uno degli operatori di sistema abbia all'interno del suo abituale profilo la possibilità di effettuare le suddette modifiche.

È fatto divieto a tutto il personale dipendente, agli amministratori, e al personale:

- diffondere o mettere in commercio abusivamente opere dell'ingegno attraverso l'immissione delle stesse in reti telematiche;
- acquistare licenze di software gestionale per conto della Società senza la prescritta autorizzazione;
- duplicare licenze di software in uso a Techem;
- trasferire su supporti Techem il contenuto di una banca dati sottratta ad una società concorrente.

I Destinatari coinvolti nelle attività legate alla gestione dei sistemi informatici dovranno ispirarsi ai seguenti principi:

- adozione di un processo formale di approvazione per l'assegnazione dei software da installare;
- adozione di regole per il corretto utilizzo di internet e posta elettronica che prevedano meccanismi volti a bloccare il download, la ricezione e l'invio di allegati di particolare tipologia (es. .mp3, .exe, ecc.);
- adozione di un processo di inventariazione e controllo del software aziendale, incluse le licenze d'uso;

- disciplina di accesso alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni, esclusivamente agli utenti (interni ed esterni) autorizzati e la loro autenticazione individuale tramite codice identificativo e password;
- adozione di meccanismi atti a impedire l'installazione, da parte degli utenti, di software sulla propria postazione di lavoro.

7.9 Reato di impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare

L'articolo 2 del D.Lgs. 16 luglio 2012, n. 109 (recante "Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare") ha introdotto nel Decreto l'articolo 25-duodecies, rubricato "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare", prevedendo la responsabilità amministrativa degli enti per il reato previsto dall'art. 22, comma 12-bis del D.Lgs. n. 286/1998 (Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero, c.d. Testo Unico Immigrazione).

Di seguito si indica la fattispecie penale richiamata dall'art. 25 duodecies del Decreto.

- Articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286. Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000,00 euro per ogni lavoratore impiegato. Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà: a) se i lavoratori occupati sono in numero superiore a tre; b) se i lavoratori occupati sono minori in età non lavorativa; c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale (NDR: ovvero a "situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro").

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori, e dipendenti della Società, nonché da Collaboratori Esterni.

L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle "aree a rischio", si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi del Reato di impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare.

AREE A RISCHIO

Con riferimento specifico al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, ai fini della presente Parte Speciale, in sede di mappatura è stata individuata la seguente area a rischio:

- SELEZIONE/ASSUNZIONE/GESTIONE (IN TERMINE DI DEFINIZIONE DELLA POLITICA RETRIBUTIVA) DELLE RISORSE UMANE.

DISPOSIZIONI E PRINCIPI SPECIFICI

Si indicano qui di seguito le disposizioni ed i principi specifici che, in relazione all'area a rischio devono essere rispettati da tutti i Destinatari ad integrazione delle altre procedure aziendali esistenti.

È fatto assoluto divieto ai Destinatari del presente Modello di porre in essere comportamenti:

- tali da integrare la fattispecie di reato sopra considerata (art.25 duodecies del Decreto);
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quella sopra considerata, possano potenzialmente diventarlo;
- non in linea o non conformi con i principi e le prescrizioni contenute nel presente Modello e nel Codice Etico.

I Destinatari dovranno:

- rispettare le regole e le prescrizioni di cui al presente Modello, al Codice Etico ed al Regolamento Aziendale;

- tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla assunzione e gestione delle risorse umane;
- rispettare le eventuali policy adottate dalla Società contenenti i principi cui attenersi al fine del rispetto delle prescrizioni anche procedurali previste dalla normativa sull'immigrazione ed il monitoraggio costante del rispetto delle stesse;
- verificare, per il tramite di pareri legali o di altri professionisti, l'eventualità che una condotta della Società possa configurare un reato previsto dal Testo Unico Immigrazione;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuto o sospettato lo svolgimento di attività illecite con riferimento alle fattispecie penali punite dal "Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero" e, in generale, dalla normativa sulla immigrazione;
- mantenere sempre un comportamento collaborativo con gli Organismi di Vigilanza e le autorità giudiziarie;
- sottoporre all'attenzione del superiore gerarchico e/o dell'ODV eventuali situazioni di incertezza in ordine ai comportamenti da tenere, all'interpretazione della normativa vigente e delle procedure interne, nonché eventuali violazioni delle norme e eventuali operazioni insolite o sospette;

In caso di assunzione di cittadini di paesi terzi (ovvero in caso di distacco di lavoratori di paesi terzi) non in possesso del permesso di soggiorno, la Società dovrà provvedere:

- alla richiesta nominativa di nulla osta (autorizzazione all'assunzione) da presentare presso l'ufficio della Prefettura competente territorialmente;
- a consegnare il nulla osta, una volta rilasciato, al cittadino che si intende assumere, affinché lo stesso possa richiedere ai competenti uffici il rilascio del visto di

ingresso per motivi di lavoro subordinato e quindi, a seguito dell'ingresso in Italia, il permesso di soggiorno;

- a farsi consegnare il permesso di soggiorno o la copia della domanda di rilascio del permesso di soggiorno presentata all'ufficio postale e la relativa ricevuta;
- ad archiviare copia della documentazione di cui al punto che precede unitamente al contratto di lavoro;
- a provvedere alle comunicazioni previste per legge al Centro per l'impiego e agli altri Enti competenti, assicurando che le informazioni trasmesse siano veritiere, complete e basate su idonea documentazione.

I Destinatari competenti dovranno:

- monitorare le scadenze dei permessi di soggiorno e degli eventuali rinnovi dei lavoratori di paesi terzi assunti alle dipendenze;
- inviare comunicazioni ai lavoratori di paesi terzi in prossimità della scadenza del permesso di soggiorno;
- verificare, in corso di rapporto di lavoro, la presentazione, da parte del lavoratore straniero, della domanda di rinnovo del permesso di soggiorno;
- prevedere l'impegno del lavoratore assunto dalla Società di trasmettere alla Società qualunque comunicazione, lettera e richiesta proveniente dalle Autorità e uffici competenti (Questura, Prefettura, Centro per l'Impiego) in merito alla validità o scadenza del permesso di soggiorno;

7.10 Reati ambientali

Il Decreto prevede una serie di Reati ambientali. In sede di mappatura è stato rilevato rischio con specifico riferimento alla seguente fattispecie:

- Gestione di rifiuti non autorizzata (art. 256 D.Lgs. 152/2006) – raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, non pericolosi e pericolosi, in mancanza della prescritta autorizzazione, iscrizione o comunicazione (art. 256, co. 1, lett. a) e b) – realizzazione o gestione di una discarica non autorizzata (art. 256, co. 3, primo periodo) – attività non consentite di miscelazione di rifiuti (art. 256, co. 5).

PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Il presente paragrafo si riferisce ai comportamenti posti in essere da amministratori e dipendenti della Società, nonché da Collaboratori Esterni.

L'obiettivo è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle "aree a rischio", si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati ambientali.

In particolare, il presente paragrafo ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'ODV, ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

In particolare, nell'espletamento delle attività considerate "a rischio", i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati ambientali;

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

AREE A RISCHIO

In sede di mappatura è stata identificata la seguente attività a rischio di compimento di reati/illeciti amministrativi riconducibili a reati di criminalità informatica:

- SMALTIMENTO RIFIUTI

DISPOSIZIONI E PRINCIPI SPECIFICI

Si indicano qui di seguito le disposizioni ed i principi specifici che, in relazione all'area a rischio devono essere rispettati da tutti i Destinatari ad integrazione delle altre procedure aziendali esistenti.

SMALTIMENTO RIFIUTI

Dall'analisi effettuata sulla documentazione raccolta, si rileva che la Società, in merito allo smaltimento dei rifiuti, ha stipulato convenzioni per la fornitura del servizio di raccolta, trasporto e smaltimento rifiuti con società di primaria importanza.