

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO
8 GIUGNO 2001, N. 231

Predisposizione: STAR SRL – Cabiato

Data: Marzo 2009

Adozione da parte del CdA:

Data: 22.04.2009

Aggiornamento: Studio Legale LCG - Milano

Data: Novembre 2010

Approvazione aggiornamento e adozione da parte del CdA:

Data: 13.12.2010



INDICE

1 - DESCRIZIONE DEL QUADRO NORMATIVO	5
1.1 INTRODUZIONE.....	5
1.2 FATTISPECIE DI REATO E REATI SENSIBILI.....	6
1.3 MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO.....	8
1.4 CODICI DI COMPORTAMENTO PREDISPOSTI DALLE ASSOCIAZIONI RAPPRESENTATIVE DI CATEGORIA	10
2 - DESCRIZIONE DELLA REALTÀ AZIENDALE	16
2.1 ATTIVITÀ DELLA SOCIETÀ.....	16
2.2 DESCRIZIONE SINTETICA DELLA STRUTTURA SOCIETARIA.....	16
2.3 GLI STRUMENTI DI GESTIONE DI TECNOLOGIE D'IMPRESA.....	16
2.4 IL CODICE ETICO O DI COMPORTAMENTO (CFR. ALLEGATO B).....	17
3 - MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO E METODOLOGIA SEGUITA PER LA SUA PREDISPOSIZIONE	18
3.1 PREMessa	18
3.2 IL PROGETTO DI TECNOLOGIE D'IMPRESA PER LA DEFINIZIONE DEL PROPRIO MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS 231/2001 E SUO SVILUPPO	18
4 - L'ORGANISMO DI VIGILANZA AI SENSI DEL D.LGS. 231/2001.....	24
4.1 L'ORGANISMO DI VIGILANZA DI TECNOLOGIE D'IMPRESA S.P.A.	24
4.1.1 Principi generali in tema di istituzione, nomina e sostituzione dell'Organismo di Vigilanza.....	25
4.2 FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA.....	26
4.3 OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA – FLUSSI INFORMATIVI	28
4.3.1 Raccolta e conservazione delle informazioni	29
4.4 REPORTING DELL'ORGANISMO DI VIGILANZA VERSO GLI ORGANI SOCIETARI.....	29
5 - SISTEMA DISCIPLINARE E SANZIONATORIO	31
5.1 FUNZIONE DEL SISTEMA DISCIPLINARE.....	31
5.2 MISURE NEI CONFRONTI DI LAVORATORI SUBORDINATI (IN GENERE COMPRESI I PREPOSTI)	31
5.3 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI.....	32
5.4 MISURE NEI CONFRONTI DEI SINDACI	33
5.5 MISURE NEI CONFRONTI DI PARTNER COMMERCIALI, CONSULENTI E COLLABORATORI ESTERNI ED IMPRESE TERZE	33
5.6 MISURE A CARICO DI DATORE DI LAVORO E/O DIRIGENTI DELEGATI.....	33
6 - PIANO DI FORMAZIONE E COMUNICAZIONE.....	35
6.1 PREMessa	35
6.2 DIPENDENTI.....	35
6.3 GESTIONE INFORMAZIONE, FORMAZIONE ED ADDESTRAMENTO	36
7 - ADOZIONE DEL MODELLO – CRITERI DI AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO	37
7.1 AGGIORNAMENTO ED ADEGUAMENTO	37
PRINCIPI DI RIFERIMENTO DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO.....	38
EX D.LGS. 231/2001	38
PARTE SPECIALE.....	38
1. FINALITÀ.....	39
2. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001	40
3. DIVIETI	40
4. LE "ATTIVITÀ SENSIBILI" AI FINI DEL D.LGS. 231/2001.....	42



- 5.1 Principi generali di controllo..... **Errore. Il segnalibro non è definito.**
- 5.2 I PROTOCOLLI SPECIFICI DI CONTROLLO..... **ERRORE. IL SEGNALIBRO NON È DEFINITO.**



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/2001

PARTE GENERALE



1 - DESCRIZIONE DEL QUADRO NORMATIVO

1.1 Introduzione

Con il decreto legislativo 8 giugno 2001 n. 231 (di seguito, il “D.Lgs. 231/2001”), emanato in attuazione della delega conferita al Governo con l’art. 11 della Legge 29 settembre 2000, n. 300¹ è stata dettata la “disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” per gli illeciti amministrativi dipendenti da reato.

Il D.Lgs. 231/2001 trova la sua genesi in alcune convenzioni internazionali e comunitarie ratificate dall’Italia che impongono di prevedere forme di responsabilità degli enti per talune fattispecie di reato, tassativamente indicate.

Secondo la disciplina introdotta dal D.Lgs. 231/2001, infatti, le società possono essere ritenute “responsabili” per alcuni reati dolosi commessi o tentati, nell’interesse o a vantaggio delle società stesse, da esponenti dei vertici aziendali (i c.d. soggetti “in posizione apicale” o semplicemente “apicali”) e da coloro che sono sottoposti alla direzione o vigilanza di questi ultimi (art. 5, comma 1, del D.Lgs. 231/2001)².

La responsabilità amministrativa delle società – che si estende ai reati commessi all’estero (purché alla loro repressione non proceda lo Stato del luogo in cui sono stati commessi) - è autonoma rispetto alla responsabilità penale e civile della persona fisica che ha commesso il reato e si affianca a quest’ultima.

Tale ampliamento di responsabilità mira sostanzialmente a coinvolgere nella punizione di determinati reati il patrimonio delle società e, in ultima analisi, gli interessi economici dei soci, i quali, fino all’entrata in vigore del decreto in esame, non pativano conseguenze dirette dalla realizzazione di reati commessi, nell’interesse o a vantaggio della loro società, da amministratori e/o dipendenti.

Secondo quanto disposto dal D.Lgs. 231/2001 alle società sono applicabili, in via diretta ed autonoma, sanzioni di natura sia pecuniaria che interdittiva in relazione a reati ascritti a soggetti funzionalmente legati alla società ai sensi dell’art. 5 del decreto.

La responsabilità amministrativa della società è, tuttavia, esclusa se la società ha, tra l’altro, adottato ed efficacemente attuato, prima della commissione dei reati, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi.

¹ Il D.Lgs. 231/2001 è pubblicato sulla Gazzetta Ufficiale del 19 giugno 2001, n. 140, la Legge 300/2000 sulla Gazzetta Ufficiale del 25 ottobre 2000, n. 250.

² Art. 5, comma 1, del D.Lgs. 231/2001: “Responsabilità dell’ente – L’ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)”.



La responsabilità amministrativa della società è, in ogni caso, esclusa se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi³.

1.1 Fattispecie di reato e Reati Sensibili

In base al D.Lgs. 231/2001, l'ente può essere ritenuto responsabile soltanto per i reati espressamente richiamati dagli artt. 24, 24-bis, 24-ter, 25, 25-bis, 25-bis.1, 25-ter, 25-quater, 25-quater.1, 25-quinquies, 25-sexies, 25-septies e 25-octies, 25 nonies e 25 decies del D.Lgs. 231/2001, se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati ex art. 5, comma 1, del decreto stesso⁴.

Le fattispecie di reato richiamate dal D.Lgs. 231/2001 possono essere comprese, per comodità espositiva, nelle seguenti categorie:

- delitti nei rapporti con la Pubblica Amministrazione (quali ad esempio corruzione, concussione, malversazione ai danni dello Stato, truffa ai danni dello Stato e frode informatica ai danni dello Stato, richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001)⁵;
- delitti di criminalità organizzata (quali ad esempio i reati di associazione per delinquere, scambio elettorale politico-mafioso, sequestro di persona a scopo di estorsione, richiamati dall'art. 24 *ter* del D.Lgs. 231/2001)⁶;
- delitti contro la fede pubblica (quali ad esempio falsità in monete, carte di pubblico credito e valori di bollo e in strumenti o segni di riconoscimento, richiamati dall'art. 25 *bis* D.Lgs. 231/2001)⁷;

³ Art. 5, comma 2, del D.Lgs. 231/2001: "Responsabilità dell'ente – L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi".

⁴ L'articolo 23 del D. Lgs. 231/2001 prevede inoltre la punibilità dell'ente qualora, nello svolgimento dell'attività dello stesso ente a cui è stata applicata una sanzione o una misura cautelare interdittiva, siano trasgrediti gli obblighi o i divieti inerenti a tali sanzioni e misure.

⁵ Si tratta dei reati seguenti: malversazione a danno dello Stato o dell'Unione europea (art. 316-bis c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.), truffa aggravata a danno dello Stato (art. 640, comma 2, n. 1, c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.), frode informatica a danno dello Stato o di altro ente pubblico (art. 640-ter c.p.), corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318, 319 e 319-bis c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), istigazione alla corruzione (art. 322 c.p.), concussione (art. 317 c.p.), corruzione, istigazione alla corruzione e concussione di membri delle Comunità europee, funzionari delle Comunità europee, degli Stati esteri e delle organizzazioni pubbliche internazionali (art. 322-bis c.p.).

⁶ L'art. 24 *ter* è stato introdotto dall'art. 2, comma 29, della legge 15 luglio 2009 n. 94; vengono richiamati i reati di associazione per delinquere (art. 416 c.p.), associazioni di tipo mafioso anche straniere (art. 416 bis c.p.), scambio elettorale politico mafioso (art. 416 *ter* c.p.), sequestro di persona a scopo di estorsione (art. 630 c.p.).

⁷ L'art. 25-bis è stato introdotto nel D.Lgs. 231/2001 dall'art. 6 del D.L. 350/2001, convertito in legge, con modificazioni, dall'art. 1 della L. 409/2001. Si tratta dei reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.), alterazione di monete (art. 454 c.p.), spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.), spendita di monete falsificate ricevute in buona fede (art. 457 c.p.), falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.), contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.), fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.), uso di valori di bollo contraffatti o alterati (art. 464 c.p.), Contraffazione,



- delitti contro l'industria e il commercio (quali ad esempio illecita concorrenza con minaccia o violenza, frode nell'esercizio del commercio, vendita di sostanze alimentari non genuine come genuine, richiamati dall'art. 25-bis.1)⁸;
- reati societari (quali ad esempio false comunicazioni sociali, impedito controllo, illecita influenza sull'assemblea, richiamati dall'art. 25 *ter* D.Lgs. 231/2001 da ultimo modificato con la legge 262/2005)⁹;
- delitti in materia di terrorismo e di eversione dell'ordine democratico (richiamati dall'art. 25 *quater* del D.Lgs. 231/2001);
- delitti contro la personalità individuale (quali ad esempio la tratta di persone, la riduzione e mantenimento in schiavitù, richiamati dall'art. 25 *quater*.1 e dall'art. 25 *quinquies* D.Lgs. 231/2001)¹⁰;
- delitti di abuso di mercato (abuso di informazioni privilegiate e manipolazione del mercato, richiamati dall'art. 25 *sexies* D.Lgs. 231/2001)¹¹;
- reati transnazionali (quali ad esempio l'associazione per delinquere ed i reati di intralcio alla giustizia, sempre che gli stessi reati presentino il requisito della "transnazionalità")¹²;

alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.), Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

⁸ L'art. 25-bis.1. è stato inserito dall'art. 17, comma 7, lettera b), della legge 23 luglio 2009, n. 99; si tratta in particolare dei delitti di turbata libertà dell'industria o del commercio (art. 513 c.p.), illecita concorrenza con minaccia o violenza (art. 513 bis), frodi contro le industrie nazionali (art. 514 c.p.), frode nell'esercizio del commercio (art. 515 c.p.), vendita di sostanze alimentari non genuine come genuine (art.516 c.p.), vendita di prodotti industriali con segni mendaci (art. 517 c.p.), fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 *ter*), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 *quater*), Art.4 L. 350/03.

⁹ L'art. 25-*ter* è stato introdotto nel D.Lgs. 231/2001 dall'art. 3 del D.Lgs. 61/2002. Si tratta dei reati di false comunicazioni sociali e false comunicazioni sociali in danno dei soci o dei creditori (artt. 2621 e 2622 c.c.), falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.), impedito controllo (art. 2625, 2° comma, c.c.), formazione fittizia del capitale (art. 2632 c.c.), indebita restituzione dei conferimenti (art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (art. 2627 c.c.), illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.), operazioni in pregiudizio dei creditori (art. 2629 c.c.), omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), illecita influenza sull'assemblea (art. 2636 c.c.), agiotaggio (art. 2637 c.c.), ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

¹⁰ L'art. 25-*quinquies* è stato introdotto nel D.Lgs. 231/2001 dall'art. 5 della legge 11 agosto 2003, n. 228. Si tratta dei reati di riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.), tratta di persone (art. 601 c.p.), acquisto e alienazione di schiavi (art. 602 c.p.), reati connessi alla prostituzione minorile e allo sfruttamento della stessa (art. 600-bis c.p.), alla pornografia minorile e allo sfruttamento della stessa (art. 600-*ter* c.p.), detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori (art. 600-*quater* c.p.), iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.).

L'art. 25-*quater*.1 è stato introdotto dalla legge 9 gennaio 2006 n. 7 e si riferisce al delitto di mutilazione di organi genitali femminili (art. 583 bis c.p.)

¹¹ L'art. 25-*sexies* è stato introdotto nel D.Lgs. 231/2001 dall'art. 9, comma 3, della legge 62/2005. Si tratta dei reati di abuso di informazioni privilegiate (art. 184 D.Lgs. 58/1998) e manipolazione del mercato (art. 185 D.Lgs. 58/1998).

¹² I reati transnazionali non sono stati inseriti direttamente nel D.Lgs. 231/2001 ma tale normativa è ad essi applicabile in base all'art.10 della legge 146/2006. Ai fini della predetta legge si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia



- reati in materia di salute e sicurezza sui luoghi di lavoro (omicidio colposo e lesioni personali gravi colpose richiamati dall'art. 25 *septies* D.Lgs. 231/2001)¹³;
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (richiamati dall'art. 25 *octies* D.Lgs. 231/01)¹⁴;
- delitti informatici e trattamento illecito di dati (art. 24 *bis*, D.Lgs. 231/01)¹⁵;
- delitti in materia di violazione del diritto d'autore (art. 25 *nonies* D.Lgs. 231/01)¹⁶;
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies* D.Lgs. 231/01).

1.3 Modelli di organizzazione, gestione e controllo

Aspetto caratteristico del D.Lgs. 231/01 è l'attribuzione di un valore esimente ai modelli di organizzazione, gestione e controllo della società. In caso di reato commesso da un soggetto in posizione apicale, infatti, la società non risponde se prova che (art. 6, comma 1, del D.Lgs. 231/2001):

- 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 quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo della società dotato di autonomi poteri di iniziativa e di controllo;

commesso in uno Stato ma abbia effetti sostanziali in un altro Stato. Si tratta dei reati di associazione per delinquere (art. 416 c.p.), associazione di tipo mafioso (art. 416-bis c.p.), associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater d.p.r. 43/1973), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 d.p.r. 309/1990), disposizioni contro le immigrazioni clandestine (art. 12, co. 3, 3-bis, 3-ter e 5 D.Lgs. 286/1998), induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) e favoreggiamento personale (art. 378 c.p.).

¹³ L'art. 25-septies D.Lgs. 231/01 è stato introdotto dalla legge 123/07. Si tratta dei reati di omicidio colposo e lesioni colpose gravi commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (artt. 589 e 590, co. 3, c.p.).

¹⁴ L'art. 25-octies è stato introdotto nel D.Lgs. 231/2001 dall'art. 63, comma 3, del D.Lgs. 231/07. Si tratta dei reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648-bis c.p.) ed impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter).

¹⁵ L'art. 24-bis è stato introdotto nel D.Lgs. 231/01 dall'art. 7 della legge 48/2008. Si tratta dei reati di falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.), diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.), installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.), danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.), danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.) e frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

¹⁶ L'art. 25 nonies è stato inserito dall'art. 15 comma 7, lettera c), della legge 23 luglio 2009, n. 99.



- c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza;

Si ricorda che per i reati di cui art. 25 septies D.Lgs. 231/01 si rimanda anche a quanto disciplinato dall'art. 30 D.Lgs. 81/08 in materia di tutela della salute e della sicurezza nei luoghi di lavoro¹⁷.

La società dovrà, dunque, dimostrare la sua estraneità ai fatti contestati al soggetto apicale provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di riflesso, la circostanza che la commissione del reato non deriva da una propria "colpa organizzativa".

Nel caso, invece, di un reato commesso da soggetti sottoposti all'altrui direzione o vigilanza, la società risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società è tenuta.

¹⁷ 1. Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) alle attività di sorveglianza sanitaria;
- e) alle attività di informazione e formazione dei lavoratori;
- f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge; h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

2. Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

3. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

4. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

5. In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 5-bis. La commissione consultiva permanente per la salute e sicurezza sul lavoro elabora procedure semplificate per la adozione e la efficace attuazione dei modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali.

6. L'adozione del modello di organizzazione e di gestione di cui al presente articolo nelle imprese fino a 50 lavoratori rientra tra le attività finanziabili ai sensi dell'articolo 11.



In ogni caso, la violazione degli obblighi di direzione o vigilanza è esclusa se la società, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

L'art. 7, comma 4, del D.Lgs. 231/2001 definisce, inoltre, i requisiti dell'efficace attuazione dei modelli organizzativi:

- la verifica periodica e l'eventuale modifica del modello quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione e nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il D.Lgs. 231/2001 (art. 6, comma 2) delinea il contenuto dei modelli di organizzazione e di gestione prevedendo che gli stessi, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, devono:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- estendere per la parte reati salute e sicurezza quanto previsto dall'art. 30 D.Lgs. 81/08 che si ritiene integralmente recepito.

1.4 Codici di comportamento predisposti dalle associazioni rappresentative di categoria

L'art. 6, comma 3, del D.Lgs. 231/2001 prevede "I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati".

Il presente Modello è stato redatto tenendo conto delle indicazioni espresse dalle linee guida di Confindustria e dalle previsioni normative contenute nel D.Lgs. 81/08, in particolare, l'art. 30.

Nelle Linee Guida, infatti, sono tracciati gli elementi costitutivi di un modello organizzativo di prevenzione dei reati idoneo allo scopo e sono definiti i principi fondamentali che devono caratterizzarlo. Esse costituiscono, quindi, l'imprescindibile punto di partenza per la corretta costruzione di un Modello, a cui gli enti devono ispirarsi per la predisposizione del proprio Modello.



Le caratteristiche indispensabili per la costruzione di un Modello efficace sono individuate nelle seguenti fasi:

1. l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D.Lgs. 231/2001;
2. la progettazione del sistema di controllo (c.d. protocolli per la programmazione della formazione ed attuazione delle decisioni dell'ente): ossia la valutazione del sistema esistente all'interno dell'ente ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi identificati. Sotto il profilo concettuale, ridurre un rischio comporta di dover intervenire (congiuntamente o disgiuntamente) su due fattori determinanti: la probabilità di accadimento dell'evento e l'impatto dell'evento stesso (o gravità). Il sistema appena sopra delineato non può però, per operare efficacemente, ridursi ad attività una tantum, bensì deve tradursi in un processo continuo (o comunque svolto con una periodicità adeguata), da reiterare con particolare attenzione nei momenti di cambiamento aziendale (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, infortuni, ecc.).

Concetto base per la costruzione di un sistema di controllo preventivo, dunque, è quello di rischio accettabile che si ha qualora i controlli aggiuntivi "costino" più della risorsa da proteggere. Nel caso del D.Lgs n. 231/01 la logica economica dei costi non può essere un riferimento utilizzabile in via esclusiva. E' necessario, al fine di evitare una lista di controlli che si presenterebbe altrimenti virtualmente infinita, definire una soglia effettiva che consenta di porre un limite alla quantità/qualità alle misure di prevenzione da introdurre per evitare la commissione dei reati considerati.

In sostanza, secondo la logica del decreto stesso, la soglia di accettabilità è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente ed, infatti, l'art 6, co. 1°, lett. c) sancisce come l'ente non risponda se prova che "Le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e gestione". L'agente, dunque, non solo dovrà volere l'evento reato ma, per delinquere, deve costretto a "forzare" l'insieme delle misure di prevenzione adottate dall'ente.

Come già accennato la gestione dei rischi è, in primo luogo, un processo che le imprese devono attivare al proprio interno di modo che i modelli organizzativi risultino essere l'applicazione delle citate indicazioni, in funzione del contesto operativo interno ed esterno dell'ente, rapportato alle singole ipotesi di reato connesse alle attività svolte. A tal fine l'ente si deve dotare di un organismo aziendale che, con la collaborazione del management di linea, svolga il processo di autovalutazione, affidato, altresì, al management operativo con il supporto di un tutore metodologico.

Il controllo interno deve essere eseguito secondo i seguenti passi operativi:

- a. Inventariazione degli ambiti aziendali di attività, attraverso il compimento di una revisione periodica ed esaustiva della realtà aziendale, finalizzata alla individuazione delle potenziali aree a rischio di reato e dei soggetti che vi operano (creazione di una mappa delle aree a rischio);



- b. Analisi dei rischi potenziali, ovvero l'analisi delle possibili modalità attuative dei reati nelle diverse aree aziendali (creazione di una mappa documentata delle potenziali modalità attuative degli illeciti nelle aree a rischio).
- c. Valutazione/costruzione/adequamento del sistema di controlli preventivi eventualmente già esistenti ed adeguamento degli stessi alle prescrizioni del decreto (descrizione documentata del sistema dei controlli preventivi attivati, con dettaglio delle singole componenti del sistema, nonché degli adeguamenti eventualmente necessari).

Rende più efficaci i controlli e facilita l'applicazione dell'esimente, peraltro, la documentazione scritta dei passi compiuti per la costruzione del modello, soprattutto in termini probatori, gravando sull'ente la dimostrazione della propria innocenza qualora i reati siano commessi da soggetti in posizione "apicale"; in caso di reati legati agli aspetti di Salute e Sicurezza dei lavoratori, la registrazione delle attività riveste peraltro carattere obbligatorio.

Secondo le indicazioni appena fornite si elencano qui di seguito le componenti ovvero i protocolli, di un sistema di controllo preventivo che devono essere attuate a livello aziendale per garantire l'efficacia del Modello e che sono così individuate da Confindustria:

- adozione di un Codice Etico o di Comportamento con riferimento ai reati considerati;
- adozione di un sistema organizzativo sufficientemente formalizzato e chiaro soprattutto per quanto concerne l'attribuzione di responsabilità;
- adozione di procedure manuali e informatiche, cercando di separare i compiti fra coloro che svolgono attività cruciali di un processo a rischio (con particolare attenzione sui flussi finanziari non rientranti nei processi tipici aziendali e con caratteri di eccezionalità e discrezionalità);
- adozione di un sistema di poteri autorizzativi e di firma;
- adozione di un sistema di comunicazione e formazione del personale tale per cui la divulgazione sia capillare, efficace, autorevole, dettagliata, chiara e periodicamente ripetuta;
- adozione di un sistema di controllo di gestione;
- la nomina dell'Organismo di Vigilanza, ossia dell'organo al quale affidare il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento;
- la previsione di un sistema disciplinare o di meccanismi sanzionatori per le violazioni delle norme del Codice Etico e delle procedure previste dal Modello.



Le componenti sopra evidenziate devono ispirarsi ai seguenti principi:

- ogni operazione, transazione, azione deve essere verificabile, documentata, coerente e congrua e l'adozione di misure di sicurezza tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- nessuno può gestire in autonomia un intero processo, per cui occorre che: 1) a nessuno vengano attribuiti poteri illimitati; 2) i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione; 3) i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate;
- il sistema di controllo deve documentare l'effettuazione dei controlli.

Si segnala che il presente Modello è stato redatto tenendo in considerazione la realtà concreta della società, la sua struttura organizzativa nonché la specifica attività prestata e gli obblighi di legge previsti. In particolare, il Modello segue le indicazioni contenute nelle "Linee guida regionali per la definizione di modelli di organizzazione, gestione e controllo degli enti accreditati che erogano servizi nell'ambito della filiera istruzione-formazione-lavoro".

"Da un punto di vista generale, si precisa innanzitutto che l'accertamento della Responsabilità Amministrativa, nonché la determinazione dell'entità e del quantum della sanzione sono attribuiti al giudice penale competente per il procedimento relativo ai reati dai quali dipende la Responsabilità Amministrativa.

L'Ente è ritenuto responsabile dei reati individuati dagli artt. 24 e ss. (ad eccezione delle fattispecie di cui all'art. 25 septies e dalle leggi speciali che hanno integrato il Decreto), anche se questi siano stati realizzati nelle forme del tentativo. In tali casi, però, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà.

Ai sensi dell'art. 26 del Decreto l'Ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

L'art. 9 del Decreto distingue le sanzioni amministrative dipendenti da reato in:

- a) sanzioni pecuniarie;
- b) sanzioni interdittive;
- c) confisca;
- d) la pubblicazione della sentenza.

Le sanzioni pecuniarie (artt. 10, 11 e 12 del Decreto)



Le sanzioni pecuniarie si applicano a tutti i casi in cui venga accertata la Responsabilità Amministrativa dell'Ente. Il Decreto, al fine di determinare l'ammontare della sanzione pecuniaria applicabile in maniera adeguata al fatto criminoso commesso, utilizza il meccanismo della "quota". Il Giudice Penale, dunque, dovrà stabilire il n. di "quote" – non inferiore a 100 e non superiore a mille (di importo compreso tra un minimo di Euro 258,23 ad un massimo di massimo di € 1.549,37) che l'Ente dovrà versare, sulla base. Il Giudice determina il numero di quote sulla base degli indici individuati dell'art. 11, comma 1°:

gravità del fatto;

grado di responsabilità dell'Ente;

attività svolta per attenuare le conseguenze del fatto-reato,

nonché in base alle condizioni economiche e patrimoniali dell'Ente.

Le sanzioni interdittive (art. 9, 2 °comma, del Decreto)

Le sanzioni interdittive, individuate dall'art. 9, 2° comma, del Decreto sono irrogabili nelle sole ipotesi tassativamente previste e solo per alcuni reati. Esse sono:

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

Al pari delle sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinati dal Giudice Penale competente. Esse, comunque, hanno una durata minima di tre mesi e massima di due anni e possono essere applicate all'Ente sia all'esito del giudizio e, quindi, accertata la colpevolezza dello stesso, sia in via cautelare, ovvero quando:

- sono presenti gravi indizi per ritenere la sussistenza della Responsabilità Amministrativa dell'Ente per un illecito amministrativo dipendente da reato;
- emergono fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede;
- l'Ente ha tratto dall'illecito un profitto di rilevante entità.

La confisca (art. 19 del Decreto)

La confisca del prezzo o del profitto del reato è una sanzione obbligatoria che consegue alla eventuale sentenza di condanna (art. 19 del Decreto).

La pubblicazione della sentenza (art. 18 del Decreto)



La pubblicazione della sentenza è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva (art. 18 del Decreto).

Sequestro (artt. 53 e 54 del Decreto)

L'Autorità Giudiziaria, inoltre, può infliggere: a) il sequestro preventivo delle cose di cui è consentita la confisca (art. 53 del Decreto); b) il sequestro conservativo dei beni mobili e immobili dell'Ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54 del Decreto).



2 - DESCRIZIONE DELLA REALTÀ AZIENDALE

2.1 Attività della Società

Tecnologie d'Impresa S.r.l. (di seguito anche "Tecnologie d'Impresa" o "Società"), opera nel settore della assistenza alle imprese e alle Organizzazioni in genere in materia Salute e Sicurezza, Ambiente e gestione dei Processi di Qualità.

Tecnologie d'Impresa fondata nel 1985, gestisce la sede di Cabiato ed opera attraverso società collegate. Tecnologie d'Impresa è una organizzazione riconosciuta di alta qualità e servizi professionalmente avanzati. Punto integrante della attività della società è la Politica Qualità, Ambiente e Sicurezza redatta ormai da più di 10 anni e rivista annualmente. I fattori competitivi cui viene attribuito particolare valore per la determinazione del successo imprenditoriale della Società sono in ordine di importanza:

- la qualità delle risorse umane;
- la qualità del servizio;
- l'organizzazione di impresa.

Per quanto rileva strettamente ai fini dell'applicazione del D.Lgs. 231/01, è importante segnalare come Tecnologie d'Impresa S.r.l. partecipi solo saltuariamente a gare per l'aggiudicazione di pubblici servizi (assistenza Salute e Sicurezza, Analisi Ambientali in genere)

2.2 Descrizione sintetica della struttura societaria

Tecnologie d'Impresa è gestita da un Consiglio di Amministrazione che ha attribuito poteri chiaramente determinati al proprio Presidente, all'Amministratore Delegato ed al Consigliere delegato.

La gestione ordinaria della Società è affidata principalmente all'Amministratore Delegato.

La legale rappresentanza della Società è affidata al Presidente, al Consigliere Delegato ed all'Amministratore Delegato nei limiti dei poteri conferiti.

2.3 Gli strumenti di gestione di Tecnologie d'Impresa

I principali strumenti di gestione di cui la Società si è dotata sono:

- lo Statuto;
- il sistema di deleghe attribuite dal Consiglio di Amministrazione al Presidente e all'Amministratore Delegato



- il Documento di Valutazione dei rischi per quanto riguarda la gestione Salute e Sicurezza ed i suoi allegati;
- il sistema di gestione della salute e sicurezza certificato secondo la normativa OHSAS 18001;
- il sistema di gestione delle tematiche ambientali certificato secondo la normativa 14001;
- il sistema di gestione della qualità certificato secondo la normativa 9001;
- il sistema di gestione del laboratorio certificato 17025;
- le procedure specifiche dei sistemi di gestione atte anche a contenere e gestire il rischio di commissione di reati;
- Il Codice Etico.

L'insieme degli strumenti di gestione adottati da Tecnologie d'Impresa (qui sopra richiamati in estrema sintesi) e delle previsioni dei rischi di reato del presente Modello consente di ricostruire, rispetto alle attività sensibili, i processi di formazione ed attuazione delle decisioni dell'ente (cfr. art. 6, comma 2 lett. b, D.Lgs. 231/01).

I sistemi di gestione, nei loro aggiornamenti periodici, costituiscono parte integrante e fondamentale del presente Modello.

2.4 Il Codice Etico o di comportamento (cfr. allegato b)

I principi e le regole contenuti nel presente Modello sono coerenti con quelli previsti dal Codice Etico di Tecnologie d'Impresa S.r.l. adottato anche in ottemperanza al D.Lgs. 231/01 e conforme alla Politica della stessa nonché alle *“Linee Guida Regionali per la definizione di modelli di organizzazione, gestione e controllo degli enti accreditati che erogano servizi nell’ambito della filiera istruzione-formazione-lavoro”*.

Il Codice Etico di Tecnologie d'Impresa, approvato dal Consiglio di Amministrazione unitamente al presente documento è reso noto a tutto il personale mediante:

- la sua affissione in luoghi accessibili al pubblico, tra cui la bacheca della Società;
- la consegna ai dipendenti e collaboratori;
- la pubblicazione sul sito internet della Società.

esprime i principi etici e di deontologia che Tecnologie d'Impresa riconosce come propri e dei quali esige l'osservanza da parte di tutti coloro che operano per il conseguimento degli obiettivi della Società.

Il Codice Etico contiene, fra l'altro, linee e principi di comportamento volti a prevenire i reati di cui al D.Lgs. 231/01 e richiama espressamente il Modello come strumento utile per operare nel rispetto delle normative.

Il Codice Etico deve quindi essere considerato come parte integrante del presente Modello e strumento fondamentale per il conseguimento degli obiettivi del Modello stesso.



3 - MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO E METODOLOGIA SEGUITA PER LA SUA PREDISPOSIZIONE

3.1 Premessa

La decisione di adottare un modello di organizzazione e gestione ex D.Lgs. 231/2001, oltre a costituire un presupposto di esenzione dalla responsabilità della Società con riferimento alla commissione di alcune tipologie di reato, è considerato dalla Società un atto di responsabilità sociale nei confronti dei propri soci, dipendenti, clienti, fornitori, oltre che della collettività.

La Società ha, quindi, inteso avviare un'attività (di seguito, "Progetto") volta a rendere il proprio modello organizzativo conforme ai requisiti previsti dal D.Lgs 231/2001 e coerente ai principi etici già radicati in Tecnologie d'Impresa.

3.2 Il Progetto di Tecnologie d'Impresa per la definizione del proprio modello di organizzazione, gestione e controllo ex D.Lgs 231/2001 e suo sviluppo

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, tra i requisiti del Modello, l'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati espressamente richiamati dal decreto. Si tratta, in altri termini, di quelle attività e processi aziendali che comunemente vengono definiti "sensibili" (di seguito, "attività sensibili" e "processi sensibili").

La fase di valutazione ha preso avvio formale con un incontro (che ha coinvolto la Direzione della Società) di introduzione al progetto e di presentazione delle attività da svolgere.

A tale riunione hanno fatto seguito incontri individuali con i soggetti coinvolti nei processi ritenuti sensibili.

In particolare, il progetto mira a:

- identificare le "aree sensibili";
- sviluppare una *Gap Analysis* sui processi e le procedure/prassi aziendali in essere;
- realizzare il Sistema di Controllo Interno (c.d. protocolli per la programmazione della formazione ed attuazione delle decisioni dell'ente) individuando, inoltre, gli elementi di riferimento per sviluppare una proposta di informativa periodica verso l'organismo di vigilanza.

Il Progetto ha quindi previsto la realizzazione di tre fasi operative distinte:



FASE I - Identificazione delle Aree Sensibili (*Risk Assessment*), ossia analisi del contesto aziendale finalizzata a evidenziare in quali attività/funzioni di Tecnologie d'Impresa si possono verificare illeciti rilevanti ai fini del D.Lgs n. 231/2001.

FASE II – Identificazione del Modello Organizzativo e di controllo “a tendere” e *Gap Analysis*, ossia (1) identificazione di un modello organizzativo e di controllo “a tendere” che rappresenta il modello ideale cui l'ente deve ispirarsi al fine di definire le modalità organizzative e di controllo che consentano di perseguire gli obiettivi di liceità, eticità e trasparenza; (2) valutazione dell'adeguatezza dell'attuale modello organizzativo ai fini di prevenire tali illeciti, mettendo a confronto le regole generali contenute nel modello organizzativo di riferimento (rispondenti alle esigenze della normativa 231/2001) con le effettive modalità di svolgimento delle attività realizzate sul campo da Tecnologie d'Impresa, così come tracciate dalla prassi aziendale (3) redazione di una *Gap Analysis* che contenga i disallineamenti tra il modello a tendere e quello esistente.

FASE III - Realizzazione del sistema di controllo interno, che consiste nell'adeguamento del modello esistente ai sensi del D.Lgs n. 231/2001 e nella formulazione di indicazioni in merito ai flussi informativi verso l'organismo di vigilanza.

3.2.1 FASE I - Identificazione delle “Aree Sensibili” (Risk Assessment)

La Fase I del progetto è consistita nell'Analisi delle attività nell'ambito delle quali possono essere commessi i reati previsti dal D.Lgs n. 231/2001 (di seguito «attività sensibili») e delle funzioni aziendali coinvolte.

Tale attività ha consentito di analizzare e formalizzare, per ogni area/attività sensibile individuata, le modalità di svolgimento, le funzioni e i ruoli/responsabilità dei soggetti coinvolti, gli elementi di controllo esistenti, al fine di verificare in quali aree/settori di attività e secondo quali modalità si potessero astrattamente realizzare le fattispecie di reato di cui al D.Lgs. 231/2001.

E' stata svolta, altresì, un'analisi della documentazione societaria ed organizzativa (organigrammi, procure e deleghe, bilanci, procedure, etc.) al fine di meglio comprendere l'attività e di identificare gli ambiti aziendali oggetto dell'intervento. Si è quindi proceduto a intervistare i soggetti chiave nell'ambito della struttura aziendale coinvolti nei processi sensibili.

L'obiettivo raggiunto è stato quello di:

- Analizzare il contesto aziendale, al fine di identificare i processi/attività sensibili
- Individuare le modalità attraverso cui possono essere commessi i reati ex D. Lgs. 231/01.



- rilevare il sistema di controllo e delle relative criticità.

3.2.2 FASE II - Identificazione del Modello Organizzativo e di controllo “a tendere” e Gap Analysis

Lo svolgimento della fase II è consistita nell'identificazione di un modello organizzativo “a tendere” volto all'attuazione dei sistemi e strumenti di governo atti a garantire l'efficacia del modello. I sistemi e gli strumenti atti a garantire il governo dell'organizzazione e il funzionamento dell'ente, possono essere, a titolo esemplificativo i seguenti:

- **Statuto** - in conformità con le disposizioni di legge vigenti, contempla diverse previsioni relative al governo dell'ente volte ad assicurare il corretto svolgimento dell'attività di gestione.
- **Sistema organizzativo** - la redazione di un Sistema organizzativo, consente in ogni momento, di comprendere la struttura dell'ente, la ripartizione delle fondamentali responsabilità ed anche l'individuazione dei soggetti cui dette responsabilità sono affidate.
- **Sistema delle deleghe e delle procure** - che stabilisce, mediante l'assegnazione di specifiche procure, i poteri per rappresentare o impegnare l'ente, e, attraverso il sistema di deleghe, le responsabilità per quanto concerne gli aspetti in tema di qualità ambiente e sicurezza. L'aggiornamento del sistema di deleghe e procure deve avvenire in occasione di revisione/modifica della Struttura organizzativa e/o degli ordini di servizio o su segnalazione delle stesse strutture dell'ente.
- **Sistema di controllo di gestione** – che è in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità.
- **Sistema di Procedure, Policy, Linee Guida** – che regolamentano in modo chiaro ed efficace i processi rilevanti dell'ente, prevedendo gli opportuni punti di controllo.
- **Sistema Qualità** - l'insieme dei documenti che descrivono i processi che rispondono ai requisiti di qualità, ambientali e di sicurezza (norme 9001, 14001 e 18001) oltre che per la gestione del laboratorio.
- **Codice Etico** - esprime i principi etici e di deontologia che l'ente riconosce come propri e sui quali richiama l'osservanza da parte di tutti coloro che operano per il conseguimento degli obiettivi dell'ente stesso.



Le componenti sopra descritte devono integrarsi organicamente in un'architettura del sistema che rispetti una serie di protocolli di controllo generali quali ad esempio:

- **Segregazione dei compiti:** il sistema deve garantire l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione, deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione. Inoltre, occorre che: *i)* a nessuno vengano attribuiti poteri illimitati; *ii)* i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione; *iii)* i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate. Tale segregazione deve essere garantita dall'intervento, all'interno di uno stesso macro processo aziendale, di più soggetti al fine di garantire indipendenza e obiettività dei processi. La separazione delle funzioni può essere attuata anche attraverso l'utilizzo di sistemi informatici che abilitano certe operazioni solo a persone identificate ed autorizzate. La segregazione deve essere valutata considerando l'attività sensibile nel contesto dello specifico processo di appartenenza e tenuto conto della complessità della medesima attività.
- **Tracciabilità:** per ogni operazione vi deve essere un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa e, in ogni caso, sono disciplinati con dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate. La salvaguardia di dati e procedure in ambito informatico può essere assicurata mediante l'adozione delle misure di sicurezza già previste dal D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) per tutti i trattamenti di dati effettuati con strumenti elettronici.
- **Procure e deleghe:** i poteri autorizzativi e di firma assegnati devono essere: *i)* coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; *ii)* chiaramente definiti e conosciuti all'interno dell'ente. Sono definiti i ruoli aziendali ai quali è assegnato il potere di impegnare l'ente in determinate spese specificando i limiti e la natura delle spese. L'atto attributivo di funzioni deve rispettare gli specifici requisiti eventualmente richiesti dalla legge (es. delega in materia di salute e sicurezza dei lavoratori).
- **Attività di monitoraggio:** è finalizzata all'aggiornamento periodico/tempestivo di procure, deleghe di funzioni nonché del sistema di controllo, in coerenza con il sistema decisionale e con l'intero impianto della struttura organizzativa. Infine il protocollo prevede l'esistenza di controlli di processo.



- **Regolamentazione:** deve essere prevista l'esistenza di disposizioni idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante (quali manuali di gestione, procedure, policy, linee guida e regolamenti interni, nonché disposizioni organizzative e ordini di servizio).

Sulla base delle analisi effettuate sul sistema di controllo, è stato elaborato un documento di *Gap Analysis*, mettendo a confronto le regole generali contenute nel modello organizzativo di riferimento (rispondenti alle esigenze della normativa 231/2001) con le effettive modalità di svolgimento delle attività svolte in Tecnologie d'Impresa, così come tracciate dalla prassi aziendale.

Il documento di *Gap Analysis* è finalizzato a rilevare gli standard di controllo che devono essere necessariamente rispettati per consentire alla Società di instaurare un'organizzazione che consenta di evitare la commissione di reati rilevanti ai fini del D.Lgs. 231/2001.

3.2.3 FASE III - Realizzazione del Modello Organizzativo

Lo svolgimento della Fase III del progetto ha previsto lo sviluppo delle singole componenti del sistema di controllo interno così come definite dal D.Lgs 231/01 e dalle Linee Guida di categoria:

- Mappa delle attività "sensibili"
- Prassi aziendali che identificano la linea di processo delle aree "sensibili"
- Formazione e Comunicazione al Personale
- Informativa ai fornitori e ai consulenti
- Codice Etico
- Sistema Disciplinare
- Organismo di Vigilanza
- Flussi Informativi e segnalazioni nei confronti dell'Organismo di Vigilanza

Al termine dell'attività sopra descritta è stato redatto il presente Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001, articolato in tutte le sue componenti.

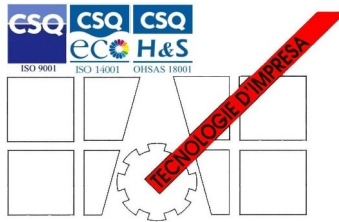
Il Modello persegue l'obiettivo di configurare un sistema strutturato ed organico volto a prevenire, per quanto possibile, la commissione di condotte che possano integrare i reati contemplati dal D.Lgs. 231/01.



Il Modello è suddiviso nella presente “**Parte Generale**”, che contiene la descrizione dell’attività svolta dalla Società e la definizione della struttura necessaria per un’effettiva ed efficace attuazione del Modello, quali il funzionamento dell’Organismo di Vigilanza, il sistema sanzionatorio, l’attività di formazione e comunicazione ed in una “**Parte Speciale**” il cui contenuto è costituito dall’individuazione delle aree sensibili con la previsione dei relativi protocolli di controllo.

Il Modello, secondo la metodologia sopra menzionata, è stato sottoposto ad attività di aggiornamento già nell’anno 2010 al fine verificare gli eventuali nuovi profili di rischio emersi nello svolgimento dell’attività lavorativa.

L’aggiornamento tiene conto anche della D.G.R. 21 dicembre 2007 n. VIII/6273 in tema di “*Erogazione dei servizi in tema di istruzione e formazione professionale nonché dei servizi per il lavoro ed il funzionamento dei relativi albi regionali – procedure e requisiti per l’accreditamento degli operatori pubblici e privati*” e delle sue successive modificazioni ed anche delle “*Linee Guida Regionali per la definizione di modelli di organizzazione, gestione e controllo degli enti accreditati che erogano servizi nell’ambito della filiera istruzione-formazione-lavoro*” in quanto Tecnologie d’Impresa svolge attività formativa che rientra in tale disciplina.



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

4.1 L'Organismo di Vigilanza di Tecnologie d'Impresa S.r.l.

In base alle previsioni del D.Lgs. 231/2001 – art. 6, comma 1, lett. a) e b) e del D.Lgs. 81/08 art. 30, l'ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 del D.Lgs. 231/2001, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello, sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate, e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità prevista dal D.Lgs. 231/2001.

I requisiti principali dell'Organismo di Vigilanza, così come proposti dalle Linee guida per la predisposizione dei Modelli di Organizzazione e Gestione emanate da Confindustria, dalle Linee Guida Regionali per la definizione di modelli di organizzazione, gestione e controllo degli enti accreditati che erogano servizi nell'ambito della filiera istruzione-formazione-lavoro e fatti propri anche dagli organi giudicanti nelle diverse pronunce giurisprudenziali pubblicate, possono essere così identificati:

- autonomia ed indipendenza: l'organismo deve essere inserito come "unità di staff in una posizione gerarchica la più elevata possibile" e deve essere previsto un riporto al Consiglio di Amministrazione. Inoltre, in capo al medesimo organismo non devono essere attribuiti compiti operativi che, per la loro natura, ne metterebbero a repentaglio l'obiettività di giudizio (ad es. evitare la nomina di chi sia direttamente coinvolto nello svolgimento di attività sensibili); l'Organismo deve avere autonomi poteri di spesa e deve poter avvalersi dell'ausilio delle funzioni societarie.
- professionalità: l'organismo deve avere un bagaglio di conoscenze, strumenti e tecniche necessari per svolgere efficacemente la propria attività. Si tratta di tecniche specialistiche proprie di chi svolge attività «ispettiva», ma anche consulenziale di analisi dei sistemi di controllo;
- continuità di azione: l'organismo deve essere in grado di garantire un'efficace e costante attuazione del modello organizzativo.

Il Consiglio di Amministrazione di Tecnologie d'Impresa identifica il proprio Organismo di Vigilanza in modo che, tenuto conto delle finalità perseguite dalla norma e dei requisiti richiesti, sia in grado di assicurare, in



relazione alle proprie dimensioni e alla propria organizzazione, l'effettività dei controlli e delle attività cui l'organismo stesso è preposto.

In ogni caso, l'Organismo di Vigilanza deve;

- avere almeno due componenti;
- avere almeno un soggetto esterno alla Società scelto per le sue competenze professionali.

4.1.1 Principi generali in tema di istituzione, nomina e sostituzione dell'Organismo di Vigilanza

L'Organismo di Vigilanza della Società è istituito con la delibera del Consiglio di Amministrazione e deve essere comunicato all'Assemblea dei Soci. L'Organismo di Vigilanza resta in carica per tre anni dalla nomina ed è rieleggibile. L'Organismo di Vigilanza cessa per scadenza del termine del periodo stabilito in sede di nomina, pur continuando a svolgere ad interim le proprie funzioni fino a nuova nomina dell'Organismo stesso che deve essere effettuata nel primo Consiglio di Amministrazione utile.

Se, nel corso della carica, un componente dell'Organismo di Vigilanza cessa dal suo incarico, il Consiglio di Amministrazione provvede alla sostituzione con propria delibera. Fino alla nuova nomina, l'Organismo di Vigilanza opera con gli altri componenti eventualmente rimasti in carica e, in mancanza, con altro soggetto nominato ad interim dal Presidente della Società.

L'eventuale compenso per la qualifica di componente dell'Organismo di Vigilanza è stabilito, per tutta la durata del mandato, dal Consiglio di Amministrazione.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza di requisiti soggettivi di eleggibilità.

In particolare, all'atto del conferimento dell'incarico, i soggetti designati a ricoprire la carica di componente dell'Organismo di Vigilanza devono rilasciare una dichiarazione nella quale attestino l'assenza di motivi di ineleggibilità quali:

- la carica di amministrazione nei tre esercizi precedenti alla nomina quale componente dell'Organismo di Vigilanza – in imprese sottoposte a fallimento, liquidazione coatta amministrativa o altre procedure concorsuali;
- condanna, anche con sentenza non passata in giudicato ed anche ai sensi dell'art. 444 c.p.p., in Italia o all'estero, per i delitti richiamati dal D.Lgs. 231/2001 o delitti comunque incidenti sull'etica professionale;
- condanna, con sentenza anche non passata in giudicato, ovvero con provvedimento che comunque ne accerti la responsabilità, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi a carico di un soggetto nominato, questi decadrà automaticamente dalla carica.



L'Organismo di Vigilanza potrà giovare – sotto la sua diretta sorveglianza e responsabilità – nello svolgimento dei compiti affidatigli della collaborazione di tutte le funzioni e strutture della Società ovvero di consulenti esterni, avvalendosi delle rispettive competenze e professionalità. Tale facoltà consente all'Organismo di Vigilanza di assicurare un elevato livello di professionalità e la necessaria continuità di azione.

A tal fine il Consiglio di Amministrazione assegna, ogni anno, un budget di spesa all'Organismo di Vigilanza tenuto conto delle richieste di quest'ultimo che dovranno essere formalmente presentate al Consiglio di Amministrazione.

L'assegnazione del budget permette all'Organismo di Vigilanza di operare in autonomia e con gli strumenti opportuni per un efficace espletamento del compito assegnatogli dal presente Modello, secondo quanto previsto dal D.Lgs. 231/2001.

Al fine di garantire la necessaria stabilità ai membri dell'Organismo di Vigilanza, la revoca dei poteri propri dell'Organismo di Vigilanza e l'attribuzione di tali poteri ad altro soggetto potrà avvenire soltanto per giusta causa mediante un'apposita delibera del Consiglio di Amministrazione e sentito il Collegio Sindacale.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di componente dell'Organismo di Vigilanza potrà intendersi, a titolo meramente esemplificativo:

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico quale (a titolo meramente esemplificativo): l'omessa redazione della relazione informativa semestrale al Consiglio di Amministrazione sull'attività svolta, di cui al successivo paragrafo 4.4;
- l'"omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza – secondo quanto previsto dall'art. 6, comma 1, lett. d), D.Lgs. 231/2001 – risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del D.Lgs. 231/2001 ovvero da provvedimento che comunque ne accerti la responsabilità;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'Organismo di Vigilanza.

In casi di particolare gravità, il Consiglio di Amministrazione potrà comunque disporre – sentito il parere del Collegio Sindacale – la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un Organismo ad interim.

4.2 Funzioni e poteri dell'Organismo di Vigilanza

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura della Società, fermo restando però che il Consiglio di Amministrazione è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo operato, in quanto ha la responsabilità ultima del funzionamento e dell'efficacia del Modello.



All'Organismo di Vigilanza sono conferiti i poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del D.Lgs. 231/2001.

Pertanto, a tale Organismo è affidato il compito di vigilare in generale:

- sulla reale (e non meramente formale) efficacia del Modello e sulla sua adeguatezza rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il D.Lgs. 231/01;
- sull'osservanza delle prescrizioni del Modello da parte dei destinatari;
- sull'aggiornamento del Modello nel caso in cui si riscontrassero esigenze di adeguamento in relazione alle mutate condizioni aziendali o normative.

In particolare, all'Organismo di Vigilanza sono affidati, per l'espletamento e l'esercizio delle proprie funzioni, i seguenti compiti e poteri:

- effettuare verifiche mirate su specifiche attività a rischio avendo libero accesso presso tutte le funzioni della Società onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal Decreto;
- promuovere l'aggiornamento della mappatura dei rischi in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal D.Lgs 231/2001;
- monitorare le iniziative di informazione/formazione finalizzate alla diffusione della conoscenza e della comprensione del Modello in ambito aziendale promosse dalla funzione competente;
- raccogliere e gestire le informazioni necessarie a fornire un quadro costantemente aggiornato circa l'attuazione del Modello;
- esprimere, sulla base delle risultanze emerse dalle attività di verifica e di controllo, una valutazione periodica sull'adeguatezza del Modello rispetto alle prescrizioni del D.Lgs 231/2001, ai principi di riferimento, alle novità normative ed agli interventi giurisprudenziali di rilievo, nonché sull'operatività dello stesso;
- segnalare all'Amministratore Delegato eventuali violazioni di protocolli o le carenze rilevate in occasione delle verifiche svolte, affinché questi possa adottare i necessari interventi di adeguamento coinvolgendo, ove necessario, il Consiglio di Amministrazione;
- vigilare sull'applicazione coerente delle sanzioni previste dalle normative interne nei casi di violazione del Modello, ferma restando la competenza dell'organo deputato per l'applicazione dei provvedimenti sanzionatori;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni.

Il Consiglio di Amministrazione della Società curerà l'adeguata comunicazione alle strutture aziendali dei compiti dell'Organismo di Vigilanza e dei suoi poteri.



L'Organismo di Vigilanza è tenuto al vincolo di riservatezza rispetto a tutte le informazioni di cui venisse a conoscenza in ragione del suo incarico.

La divulgazione di tali informazioni potrà essere effettuata solo ai soggetti e con le modalità previste dal presente Modello.

4.3 Obblighi di informazione nei confronti dell'Organismo di Vigilanza – Flussi informativi

L'Organismo di Vigilanza deve essere tempestivamente informato, mediante apposito sistema di comunicazione inviando le stesse tramite lettera all'indirizzo: Tecnologie d'Impresa S.r.l., via Don Minzoni 16 Cabiante – Att.ne Organismo di Vigilanza o e-mail all'indirizzo di posta elettronica dedicato, in merito ad atti, comportamenti od eventi che possano determinare una violazione del Modello o che, più in generale, siano rilevanti ai fini del D.Lgs. 231/2001.

Gli obblighi di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientrano nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 c.c.

Il corretto adempimento dell'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari.

Valgono, in proposito, le seguenti prescrizioni di carattere generale:

- devono essere raccolte eventuali segnalazioni relative: i) alla commissione, o al ragionevole pericolo di commissione, dei reati richiamati dal D.Lgs. 231/2001; ii) a “pratiche” non in linea con le norme di comportamento emanate dalla Società; iii) a comportamenti che, in ogni caso, possono determinare una violazione del Modello;
- il dipendente che intenda segnalare una violazione (o presunta violazione) del Modello può contattare il proprio diretto superiore gerarchico ovvero, qualora la segnalazione non dia esito o il dipendente si senta a disagio nel rivolgersi al suo diretto superiore per effettuare la segnalazione, riferire direttamente all'Organismo di Vigilanza;
- al fine di raccogliere in modo efficace le segnalazioni sopra descritte, l'Organismo di Vigilanza provvederà a comunicare a tutti i soggetti interessati, i modi e le forme di effettuazione delle stesse;
- l'Organismo di Vigilanza valuta discrezionalmente e sotto la sua responsabilità le segnalazioni ricevute e i casi in cui è necessario attivarsi.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso è assicurata la riservatezza dell'identità del segnalante, fatti salvi eventuali obblighi di legge che impongano di agire diversamente.

Oltre alle segnalazioni di cui sopra, devono essere inoltre obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:



- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.Lgs. 231/2001 e che possano coinvolgere la Società;
- le richieste di assistenza legale inoltrate da amministratori o dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui al D.Lgs. 231/2001;
- le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le comunicazioni inerenti modifiche organizzative e societarie.

All'Organismo di Vigilanza deve essere, infine, comunicato il sistema delle deleghe e delle procure adottato dalla Società oltre che l'organigramma aziendale e, tempestivamente, ogni successiva modifica degli stessi. L'Organismo di Vigilanza deve ricevere copia della reportistica in materia di salute e sicurezza sul lavoro.

4.3.1 Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, e relazione previste nel Modello è conservata dall'Organismo di Vigilanza in un apposito archivio riservato (informatico o cartaceo).

I componenti uscenti dell'Organismo di Vigilanza devono provvedere affinché il passaggio ai nuovi componenti della gestione dell'archivio avvenga correttamente.

4.4 Reporting dell'Organismo di Vigilanza verso gli organi societari

L'Organismo di Vigilanza riferisce in merito all'efficacia ed osservanza del Modello, ad eventuali aspetti critici emersi, alla necessità di eventuali interventi modificativi. A tal fine, l'Organismo di Vigilanza:

- comunica, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere i compiti che gli sono stati affidati;;
- comunica immediatamente eventuali problematiche scaturite dalle attività nonché le eventuali segnalazioni ricevute;
- relaziona per iscritto, con cadenza semestrale, al Consiglio di Amministrazione ed al Collegio sindacale sullo stato di attuazione del Modello, segnalando l'eventuale necessità di interventi migliorativi del medesimo.

Nell'ambito del reporting semestrale vengono affrontati i seguenti aspetti:

- controlli e verifiche svolti dall'Organismo di Vigilanza ed esito degli stessi;
- stato di avanzamento di eventuali progetti di implementazione/revisione di processi sensibili;



- eventuali innovazioni legislative o modifiche organizzative che richiedono aggiornamenti nell'identificazione dei rischi o variazioni del Modello;
- eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito di violazioni del Modello;
- altre informazioni ritenute significative;
- valutazione di sintesi sull'adeguatezza del Modello rispetto alle previsioni del D.Lgs. 231/2001.

Gli incontri con gli organi societari cui l'Organismo di Vigilanza riferisce devono essere verbalizzati. L'Organismo di Vigilanza cura l'archiviazione della relativa documentazione.



5 - SISTEMA DISCIPLINARE E SANZIONATORIO

5.1 Funzione del sistema disciplinare

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D.Lgs. 231/2001 e l'art. 30 comma 3 del D.Lgs. 81/08 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.

Pertanto, la definizione di un adeguato sistema disciplinare e sanzionatorio costituisce un presupposto essenziale per l'efficacia del modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001.

Le sanzioni previste saranno applicate ad ogni violazione delle disposizioni contenute nel Modello a prescindere dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare integri gli estremi di una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.

A questo riguardo, si precisa che l'applicazione delle sanzioni potrà pertanto avere luogo anche se i Destinatari abbiano posto esclusivamente in essere una violazione dei principi sanciti dal Modello che non concretizzino un reato ovvero non determinino una Responsabilità Amministrativa diretta dell'Ente.

5.2 Misure nei confronti di lavoratori subordinati (in genere compresi i preposti)

L'osservanza delle disposizioni e delle regole comportamentali previste dal Modello costituisce adempimento da parte dei dipendenti Tecnologie d'Impresa degli obblighi previsti dall'art. 2104, comma 2, c.c.; obblighi dei quali il contenuto del medesimo Modello rappresenta parte sostanziale ed integrante.

La violazione delle singole disposizioni e regole comportamentali di cui al Modello da parte dei dipendenti di Tecnologie d'Impresa costituisce sempre illecito disciplinare.

I provvedimenti disciplinari e sanzionatori sono irrogabili nei confronti dei lavoratori dipendenti di Tecnologie d'Impresa in conformità a quanto previsto dall'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori") ed eventuali normative speciali applicabili.

Per i dipendenti di livello non dirigenziale, tali provvedimenti sono quelli previsti dalle norme disciplinari di cui al CCNL per il settore commercio e terziario avanzato:

Le inadempienze del personale potranno essere sanzionate in rapporto alla relativa gravità con:

- a) biasimo inflitto verbalmente per le mancanze più lievi;
- b) biasimo inflitto per iscritto nei casi di recidiva delle infrazioni di cui al precedente punto 1);



- c) multa in misura non eccedente l'importo di quattro ore della normale retribuzione;
- d) sospensione dal servizio e dalla retribuzione per un massimo di giorni dieci;
- e) licenziamento disciplinare senza preavviso e con le altre conseguenze di ragione e di legge.

Costituisce illecito disciplinare ogni violazione delle condotte previste dal Modello o da questo richiamate e, in ogni caso, la commissione (anche sotto forma di tentativo) di qualsiasi illecito penale per cui è applicabile il D.Lgs 231/2001.

Per quanto concerne le condotte richieste dal Modello, si specifica, a titolo esemplificativo, che costituisce grave infrazione:

- l'inadempimento degli obblighi di informazione nei confronti dell'Organismo di Vigilanza previsti dal paragrafo 4.3;
- la mancata partecipazione alle iniziative di formazione promosse dalla Società;
- il mancato rispetto delle regole generali di comportamento;
- il mancato rispetto dei protocolli specifici di controllo previsti per le attività sensibili nella parte speciale del presente Modello ed i relativi flussi informativi.

Ad ogni notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. In particolare, nella fase di accertamento verrà previamente contestato al dipendente l'addebito e gli sarà, altresì, garantito un congruo termine di replica in ordine alla sua difesa. Una volta accertata la violazione, sarà comminata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa ed all'eventuale recidiva.

Resta inteso che saranno rispettate le procedure, le disposizioni e le garanzie previste dall'art. 7 dello Statuto dei Lavoratori e dalla normativa pattizia in materia di provvedimenti disciplinari

Ogni atto relativo al procedimento disciplinare dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

5.3 Misure nei confronti degli amministratori

L'Organismo di Vigilanza, raccolta una notizia di violazione delle disposizioni e delle regole di comportamento del Modello da parte di membri del Consiglio di Amministrazione, dovrà tempestivamente informare dell'accaduto il Collegio Sindacale e l'intero Consiglio di Amministrazione. I soggetti destinatari dell'informativa dell'Organismo di Vigilanza, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potranno assumere, secondo quanto previsto dallo Statuto, gli opportuni provvedimenti tra cui, se del caso, la convocazione dell'assemblea dei soci, al fine di adottare le misure più idonee previste dalla legge.

Si specifica, a titolo esemplificativo, che costituisce violazione dei doveri degli amministratori:



- la commissione, anche sotto forma di tentativo, di un reato per cui è applicabile il D.Lgs. 231/01 nell'espletamento delle proprie funzioni;
- l'inosservanza delle regole prescritte dal Modello;
- la mancata vigilanza sui prestatori di lavoro o partner della Società circa il rispetto del Modello e delle regole da esso richiamate;
- tolleranza di irregolarità commessa da prestatori di lavoro o partner della Società.

Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

5.4 Misure nei confronti dei sindaci

L'Organismo di Vigilanza, raccolta una notizia di violazione delle disposizioni e delle regole di comportamento del Modello da parte da parte di uno o più sindaci, dovrà tempestivamente informare dell'accaduto l'intero Collegio Sindacale e il Consiglio di Amministrazione. I soggetti destinatari dell'informativa dell'Organismo di Vigilanza, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potranno assumere, secondo quanto previsto dallo Statuto e dalla Legge, gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci, al fine di adottare le misure più idonee previste dalla legge.

5.5 Misure nei confronti di partner commerciali, consulenti e collaboratori esterni ed imprese terze

L'adozione da parte di partner commerciali, consulenti e collaboratori esterni, comunque denominati, o altri soggetti aventi rapporti contrattuali con la Società di comportamenti in contrasto con i principi stabiliti dal Modello sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali che saranno inserite nei relativi contratti.

Con tali clausole il terzo si obbliga ad adottare ed attuare efficacemente procedure aziendali e/o a tenere comportamenti idonei a prevenire la commissione, anche tentata, dei reati in relazione ai quali si applicano le sanzioni previste nel D.Lgs. 231/2001. L'inadempimento, anche parziale, di tale obbligazione, è sanzionato con la facoltà della Società di sospendere l'esecuzione del contratto e/o di recedere unilateralmente dallo stesso, anche in corso di esecuzione prevedendo eventualmente delle penali, oppure di risolvere il medesimo contratto, fatto salvo in ogni caso il diritto della Società al risarcimento degli eventuali danni subiti.

5.6 Misure a carico di Datore di lavoro e/o Dirigenti Delegati

“La violazione dei principi e delle regole di comportamento contenute nel Modello e nelle procedure aziendali da parte dei dirigenti, ovvero l'adozione, nell'ambito dei profili di rischio individuati nelle procedure, di un comportamento non conforme alle richiamate prescrizioni sarà assoggettata alla misura disciplinare più



idonea fra quelle previste dal Contratto Collettivo Nazionale di Lavoro applicabile, tra cui la risoluzione del rapporto di lavoro o la revoca dall'incarico.”



6 - PIANO DI FORMAZIONE E COMUNICAZIONE

6.1 Premessa

Tecnologie d'Impresa, al fine di dare efficace attuazione al Modello, assicura una corretta divulgazione dei contenuti e dei principi dello stesso, oltre che di quelli del Codice Etico, all'interno ed all'esterno della propria organizzazione.

A tale scopo, l'adozione del presente Modello viene comunicata a tutte le risorse aziendali alle quali deve esserne consegnata copia (su supporto cartaceo o informatico, trasmissibile anche in via telematica). Il Modello deve essere affisso in un luogo accessibile a tutti e messo a disposizione sul sito intranet della Società.

La Società promuove la comunicazione ed il coinvolgimento adeguati dei destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla salute e sicurezza sul lavoro (SSL), con particolare riguardo ai seguenti profili:

- i rischi per la sicurezza e la salute connessi all'attività aziendale;
- le misure e le attività di prevenzione e protezione adottate;
- i rischi specifici cui ciascun lavoratore è esposto in relazione all'attività svolta;
- i pericoli connessi all'uso delle sostanze e dei preparati pericolosi;
- le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori;
- la nomina dei soggetti cui sono affidati specifici compiti in materia di SSL.

A tali fini, è anche definito, documentato, implementato, monitorato e periodicamente aggiornato un programma di informazione e coinvolgimento dei Destinatari del Modello in materia di SSL, con particolare riguardo ai lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione.

Il coinvolgimento dei soggetti interessati è assicurato anche mediante la loro consultazione preventiva in occasione di apposite riunioni periodiche.

6.2 Dipendenti

Con modalità diversificate secondo il loro grado di coinvolgimento nelle attività individuate come sensibili ai sensi del D.Lgs. 231/2001, ogni dipendente è tenuto a: i) acquisire consapevolezza dei contenuti del Modello messi a sua disposizione; ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività.

Deve essere garantita ai dipendenti la possibilità di accedere e consultare la documentazione costituente il Modello ed i protocolli di controllo e le procedure aziendali ad esso riferibili. Inoltre, al fine di agevolare la comprensione del Modello, i dipendenti, sono tenuti a partecipare alle specifiche attività formative che saranno promosse dalla Società.



Idonei strumenti di comunicazione saranno adottati per aggiornare i dipendenti circa le eventuali modifiche apportate al Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

La partecipazione ai programmi di formazione è obbligatoria rispetto a tutti i destinatari della formazione stessa e deve essere documentata.

6.3 Gestione informazione, formazione ed addestramento

Oltre che curare gli aspetti informativi e divulgativi connessi al Modello, l'Organismo di Vigilanza ha il compito di curare l'attività di formazione finalizzata a diffondere un'adeguata conoscenza della normativa di cui al Decreto e delle conseguenze derivano dalla violazione delle norme ivi contenute.

In particolare, è previsto che i principi del Modello, ed in particolare quelli del Codice Etico che ne è parte, siano illustrati alle risorse aziendali attraverso apposite attività formative (ad es., corsi, seminari, questionari, ecc.), a cui è posto obbligo di partecipazione.

I corsi e le altre iniziative di formazione sui principi del Modello sono, peraltro, differenziati in base al ruolo ed alla responsabilità delle risorse interessate, ovvero mediante la previsione di una formazione più intensa e caratterizzata da un più elevato grado di approfondimento per i soggetti qualificabili come "apicali" alla stregua del Decreto, nonché per quelli operanti nelle aree qualificabili come "a rischio" ai sensi del Modello.

La Società promuove, inoltre, la formazione e l'addestramento dei Destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL, al fine di assicurare un'adeguata consapevolezza circa l'importanza sia della conformità delle azioni rispetto al Modello, sia delle possibili conseguenze connesse a violazioni dello stesso. A questo riguardo, particolare rilevanza è riconosciuta alla formazione ed all'addestramento dei soggetti che svolgono compiti in materia di SSL.

A tali fini, è definito, documentato, implementato, monitorato ed aggiornato, da parte della Società, un programma di formazione ed addestramento periodici dei Destinatari del Modello - con particolare riguardo ai lavoratori neo- assunti, per i quali è necessaria una particolare qualificazione - in materia di SSL, anche con riferimento alla sicurezza aziendale e ai differenti profili di rischio (ad esempio, squadra antincendio, pronto soccorso, preposti alla sicurezza, ecc.). In particolare, si prevede che la formazione e l'addestramento sono differenziati in base al posto di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro, di nuove tecnologie, di nuove sostanze e preparati pericolosi.



7 - ADOZIONE DEL MODELLO – CRITERI DI AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO

7.1 Aggiornamento ed adeguamento

Il Consiglio di Amministrazione delibera in merito all'aggiornamento del Modello e del suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- i)* modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- ii)* cambiamenti delle aree di business;
- iii)* modifiche normative;
- iv)* risultanze dei controlli;
- v)* significative violazioni delle prescrizioni del Modello.

Il Modello sarà, in ogni caso, sottoposto a procedimento di revisione periodica con cadenza triennale.



PRINCIPI DI RIFERIMENTO DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

EX D.LGS. 231/2001

PARTE SPECIALE



1. Finalità

La presente Sezione ha la finalità di definire linee e principi di comportamento che tutti gli esponenti aziendali (ad es.: dipendenti, amministratori, sindaci) dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività svolte in Tecnologie d'Impresa e considerate "a rischio", la commissione dei reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

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

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

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

- Statuto sociale;
- Modello Organizzativo;
- Codice Etico;
- Procure e deleghe;
- Sistemi di gestione in essere (9001, 14001, 18001 e laboratorio)
- Documento di Valutazione dei Rischi, suoi allegati e procedure per la gestione della Salute e Sicurezza dei lavoratori;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

È, inoltre, espressamente vietato adottare comportamenti contrari a quanto previsto dalla normativa vigente.



2. Le fattispecie di reato richiamate dal D.Lgs. 231/2001

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

A tal fine, si allega al presente documento (all. 1) la descrizione degli illeciti più rilevanti ai fine dell'applicazione del D.Lgs. 231/01 così come individuati dalle Linee Guida Regionali per la definizione di modelli di organizzazione, gestione e controllo degli enti accreditati che erogano servizi nell'ambito della filiera istruzione-formazione-lavoro.

In ogni caso, la Società promuove la formazione presso le proprie persone al fine di illustrare le caratteristiche dei reati rilevanti curando anche le evoluzioni normative.

3. Divieti

A prescindere da quanto previsto dai protocolli di controllo adottati dalla Società, al fine di evitare la commissione di tali reati è comunque sempre ed espressamente vietato porre in essere le seguenti condotte:

- adottare comportamenti che costituiscano un reato o che comunque siano in violazione di legge e/o di regolamenti;
- corrispondere od offrire, direttamente o indirettamente, pagamenti o benefici materiali a pubblici ufficiali o incaricati di pubblico servizio per influenzare o compensare un atto del loro ufficio (o ad esso contrario) ed assicurare vantaggi di qualunque tipo alla Società;
- utilizzare lo strumento dell'assunzione o il sistema retributivo per accordare vantaggi diretti o indiretti a pubblici ufficiali o incaricati di pubblico servizio;
- presentare dichiarazioni o informazioni non veritiere a organismi pubblici;
- destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi, o finanziamenti, a scopi diversi da quelli per cui sono state concesse;
- emettere richieste di acquisto che non trovino riscontro in una specifica e motivabile esigenza della Società e che non siano autorizzate in base alle procure conferite;
- riconoscere compensi a consulenti e fornitori che non trovino giustificazione in relazione al tipo di incarico da svolgere ed ai prezzi di mercato;
- utilizzare le risorse informatiche della Società per fini diversi da quelli connessi allo svolgimento delle attività proprie dell'impresa (in particolare è fatto rigoroso divieto di utilizzare tali strumenti per ricevere, archiviare, visionare o diffondere materiale pornografico ovvero per la diffusione di materiale od informazioni di carattere terroristico o eversivo);
- favorire l'ingresso o la permanenza nello Stato di soggetti non aventi diritto;



- intrattenere rapporti economici o commerciali con soggetti od enti che risultino essere direttamente od indirettamente coinvolti in associazioni terroristiche od eversive.

Con particolare riferimento ai reati societari richiamati dall'art. 25 ter D.Lgs. 231/01 (reati societari) è espressamente vietato

- elaborare o comunicare dati falsi o tali da fornire una descrizione non veritiera della situazione economica, patrimoniale e finanziaria della Società;
- omettere di comunicare informazioni previste dalla normativa vigente o dalle regole interne relativamente alla situazione economica, patrimoniale e finanziaria della Società;
- restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli se non nei casi previsti dalla legge;
- ripartire utili o acconti non effettivamente conseguiti o da destinarsi per legge a riserva;
- distribuire riserve nei casi in cui ciò non è consentito dalla legge;
- ridurre il capitale sociale od effettuare fusioni o scissioni violando le disposizioni di legge a tutela dei creditori;
- formare o aumentare in modo fittizio il capitale sociale;
- impedire od ostacolare lo svolgimento dell'attività di controllo da parte del Collegio Sindacale o della società preposta al controllo e alla revisione contabile e fornire dati non veritieri;
- porre in essere atti tali da alterare la regolare formazione della volontà dell'assemblea;
- omettere di comunicare la presenza di conflitti di interessi nell'esercizio della carica di amministratore nella Società o in società controllate o partecipate.



4. Le “attività sensibili” ai fini del D.Lgs. 231/2001

L’art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l’individuazione delle cosiddette attività “sensibili”, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L’analisi svolta nel corso del progetto ha permesso di individuare le attività di Tecnologie d’Impresa che potrebbero essere considerate “sensibili” con riferimento al rischio di commissione dei reati richiamati dal D.Lgs. 231/2001.

Le attività sensibili rilevate sono le seguenti:

-omissis-