FORMARE S.r.l.

Agenzia formativa di Federlazio
FORMARE

FORMARE SCARL Società consortile a responsabilità limitata con unico socio.

ESTRATTO
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
ai sensi del D.Lgs. 231/2001

Roma, 14 gennaio 2026

INDICE

FORMARE Srl

Agenzia formativa di Federlazio
FORMARE

FORMARE SCARL Società consortile a responsabilità limitata con unico socio.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D.Lgs. 231/2001

PARTE GENERALE

1 PREMESSA

Il presente Modello è stato elaborato sulla base della documentazione cartacea e delle informazioni fornite dai referenti aziendali individuati dalla Società "FORMARE Scarl - Società Consortile Mista con Attività Estrerna a responsabilità limitata a socio unico" (di seguito la "Società" o più semplicemente FORMARE S.r.l.) durante gli incontri programmati per lo sviluppo del progetto.

Il supporto metodologico della consulenza esterna, partendo dalle informazioni e delle evidenze documentali messe a disposizione dal personale della Società, ha reso possibile la redazione del presente documento, a sua volta validato ed approvato dai vertici della Società.

Per la realizzazione del presente Modello è stato costituito in FORMARE S.r.l. un Gruppo di lavoro composto da referenti aziendali, (con il supporto metodologico esterno di consulenza specialistica), avente il compito di:

- facilitare le relazioni con il personale della Società coinvolto dal progetto;
- verificare ed approvare i risultati ottenuti durante le diverse fasi del progetto;
- reperire e fornire tutte le informazioni e la documentazione necessarie allo sviluppo del presente Modello e alla realizzazione della cosiddetta "mappatura" dei rischi;
- approvare i documenti redatti durante le fasi del progetto.

2 INTRODUZIONE ALLA NORMATIVA

2.1 Il Decreto Legislativo 231 del 8 giugno 2001

Il D.Lgs. 231/2001 ha introdotto nel nostro ordinamento giuridico la "responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (definite enti), in conseguenza di reati commessi o tentati nel loro interesse o a loro vantaggio da soggetti che rivestono funzioni di rappresentanza, di amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria.

Sono soggette alla stessa normativa, altresì, le persone che esercitano anche di fatto la gestione ed il controllo dell'ente o le persone sottoposte alla direzione o vigilanza dei predetti soggetti.

Per effetto dell'entrata in vigore dell'indicata norma, gli enti possono elaborare ed adottare un sistema di prevenzione che, intervenendo sui processi, concorra a prevenire la commissione di fatti illeciti commessi da propri dipendenti e/o collaboratori, così da fungere da esimente rispetto alle sanzioni penali previste dal Decreto citato.

Trattasi della prevenzione dei cosiddetti "reati presupposto" commessi, appunto, nell'interesse dell'ente o a suo vantaggio dai soggetti specificamente sopra individuati: sono pertanto esclusi i reati commessi nell'esclusivo interesse proprio o di terzi.

Circa i concetti di "vantaggio" e di "interesse" citati dal Decreto, è possibile identificare il primo dei due concetti, quello di "vantaggio", con quello di profitto, in coerenza con lo stesso disposto del Decreto che, all'art. 6 co. 4, prevede la confisca obbligatoria del "profitto" che l'ente ha tratto dal reato. Anche l'art 12 consente la riduzione della sanzione pecuniaria se l'ente non ha ricavato un "vantaggio" o ha ricavato un vantaggio minimo dal reato. L'art 13 prevede ancora l'applicazione di sanzioni interdittive se l'ente ha tratto dal reato un "profitto" di rilevante entità. Le sanzioni interdittive non si applicano se, tra l'altro, l'ente ha messo a disposizione il "profitto" conseguito, ai fini della confisca (art 16). L'art 17 prevede poi l'applicazione in via definitiva della sanzione dell'interdizione se, tra l'altro,

l'ente ha tratto dal reato un "profitto" di rilevante entità. Infine, la confisca del prezzo o "profitto" del reato è obbligatoria nei confronti dell'ente (art 19).

A differenza del concetto di “vantaggio”, che viene valutato “ex-post”, il concetto di “interesse” viene invece valutato “ex-ante”, sulla base della finalità della condotta della persona che ha commesso il reato.

Il tipo di responsabilità prefigurata dal D.Lgs. n. 231/2001 si aggiunge inoltre alla responsabilità che fa capo alla persona singola.

In sintesi, l'art. 5 del D.Lgs. n. 231/2001 prevede che l'ente sia responsabile relativamente ai reati individuati dallo stesso Decreto, commessi nell'interesse oppure a vantaggio dell'ente da:

- soggetti apicali, come sopra definiti, ovvero
- persone sottoposte alla direzione o alla vigilanza di un apicale.

Le disposizioni in esame contengono profili di estrema rilevanza, poiché introducono la possibilità che ad un ente (ivi comprendendo in genere le persone giuridiche, le società e le associazioni, anche prive di personalità giuridica) venga ricondotta una responsabilità definita genericamente "amministrativa", ma di fatto di tipo penale, diversa, autonoma e concorrente rispetto a quella delle persone fisiche e conseguente a specifici fatti di reato commessi da componenti gli Organi Sociali o dipendenti a vantaggio dell'impresa stessa.

Va altresì osservato che tale tipo di responsabilità degli "enti" non opera "sic et simpliciter" per tutti i reati commessi da coloro che lavorano al loro interno, ma, affinché sussista, occorre che si tratti di uno dei reati specifici previsti dal Decreto stesso (“reati presupposto”), che ha subito le seguenti integrazioni normative, che hanno ampliato il novero dei reati ricompresi nell’ambito di operatività della norma in esame:

- Decreto Legge n. 350 del 25 settembre 2001, convertito con Legge n. 409 del 23 novembre 2001, recante “Disposizioni urgenti in vista dell'introduzione dell'euro, in materia di tassazione dei redditi di natura finanziaria, di emersione di attività detenute all'estero, di cartolarizzazione e di altre operazioni finanziarie”, relativo alla “Falsità in monete, in carte di pubblico credito e in valori di bollo”;
- Decreto Legislativo n. 61 dell’11 aprile 2002, in materia di false comunicazioni sociali;
- Legge n. 7 del 14 gennaio 2003, in materia di repressione del finanziamento al terrorismo;
- Legge n. 228 dell’11 agosto 2003, “Misure contro la tratta di persone”;
- Legge n. 62 del 18 aprile 2005, recante “Disposizioni per l’adempimento di obblighi derivanti dall’appartenenza dell’Italia alle Comunità europee (Legge comunitaria 2004)”, che ha introdotto tra i reati-presupposto i reati di abuso di mercato;
- Legge n. 262 del 28 dicembre 2005 in materia di tutela del risparmio, che ha modificato l’art. 25 ter del D.Lgs. 231/2001 in relazione ai reati societari;
- Legge n. 7 del 9 gennaio 2006, recante "Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile";
- Legge n. 123 del 3 agosto 2007, che ha previsto la responsabilità dell’ente per reati contro la tutela della salute e della sicurezza sul lavoro;
- Decreto Legislativo n. 231 del 21 novembre 2007 che estende la responsabilità dell’ente ai reati di ricettazione, riciclaggio ed impiego di denaro beni o utilità di provenienza illecita;

- Legge n. 48 del 18 marzo 2008 che prevede, tra i reati presupposto, i delitti informatici ed il trattamento illecito di dati;
- Decreto Legislativo n. 81 del 9 aprile 2008 che, all'art. 300, ha modificato l'art. 25-septies del Decreto;
- Legge n. 94 del 15 luglio 2009 che introduce (art. 2, co. 29) i Delitti di criminalità organizzata;
- Legge n. 99 del 23 luglio 2009 "Disposizioni per lo sviluppo e internazionalizzazione delle imprese, nonché in materia di energia", che introduce (art. 15, co. 7) i Delitti contro l'industria e il commercio ed i Delitti in materia di violazione del diritto d'autore;
- Legge n. 116 del 3 agosto 2009 che all'art. 4 introduce il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria";
- Decreto Legislativo n. 121 del 7 luglio 2011, rubricato "Attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della Direttiva 2009/123/CE che modifica la Direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni".

  Tale Decreto prevede, all'art. 2:

  - la diversa numerazione dell'art. 25 novies del D.Lgs. 231/2001 (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria) in art. 25 decies;
  - l'inserimento nel D.Lgs. 231/2001 dell'art. 25 undecies "Reati ambientali".
- Decreto Legislativo n. 109 del 25 luglio 2012, che ha introdotto l'art. 25-duodecies "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare";
- Legge n. 190 del 6 novembre 2012 rubricata "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione". Tale norma ha introdotto, tra i c.d. "reati presupposto" il reato di "Induzione indebita a dare o promettere utilità" (art. 319-quater c.p.) e il reato di "Corruzione tra privati" (art. 2635 c.c.) ed ha modificato la portata e/o il trattamento sanzionatorio di alcuni reati contro la Pubblica Amministrazione, quali la "Corruzione per un atto d'ufficio" (art. 318 c.p.), ora rubricata "Corruzione per l'esercizio della funzione", e la concussione (art. 317 c.p.), in parte confluita nel succitato nuovo reato di "Induzione indebita a dare o promettere utilità" (art. 319-quater c.p.);
- Decreto Legislativo n. 39 del 4 marzo 2014, rubricato "Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile", il quale introduce tra i "reati presupposto", in particolare nell'art. 25-quinquies, l'"adescamento di minorenni" (art. 609-undecies c.p.);
- Legge n. 186 del 15 dicembre 2014, rubricata "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di auto riciclaggio", che all'3, comma 3 inserisce nel Codice Penale l'articolo 648-ter.1 (Autoriciclaggio). Il medesimo articolo della Legge ha quindi modificato l'articolo 25-octies del Decreto, inserendo al primo comma il richiamo all'art. 648-ter.1 ed aggiungendo alla rubrica, in fine, le parole ", nonché autoriciclaggio";
- Legge n. 68 del 22 maggio 2015, "Disposizioni in materia di delitti contro l'ambiente", la quale aggiunge ai reati-presupposto dell'art. 25-undecies del Decreto: il delitto di inquinamento ambientale (art. 425-bis c.p.), il delitto di disastro ambientale (art. 452-quater c.p.), i delitti colposi contro l'ambiente (art.452-quinquies c.p.), i delitti associativi aggravati (art. 452-octies c.p.), il delitto di traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);

- Legge n. 69 del 27 maggio 2015 che, all'art. 12, ha introdotto "Modifiche alle disposizioni sulla responsabilità amministrativa degli enti in relazione ai reati societari". Questa Legge ha altresì, tra l'altro: modificato il reato di false comunicazioni sociali, introdotto il reato di false comunicazioni sociali con fatti di lieve entità; modificato il reato di false comunicazioni sociali delle società quotate; sostituito l'art. 317 del Codice Penale (Concussione);
- Decreti Legislativi n. 7 e n. 8 del 15 gennaio 2016, che hanno introdotto modifiche ai delitti informatici.
- Decreto Legislativo n. 125 del 21 giugno 2016 (Attuazione della direttiva 2014/62/UE sulla protezione mediante il diritto penale dell´euro e di altre monete contro la falsificazione) che ha introdotto modifiche agli articoli del Codice Penale relativi ai delitti di falsità in monete, carte di pubblico credito e valori di bollo (art. 25-bis del D. Lgs. 231)
- Legge n. 199 del 29 ottobre 2016, contenente disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo.
- Decreto Legislativo n. 38 del 15 marzo 2017 (Attuazione della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato), che ha introdotto modifiche alla Corruzione tra privati (art. 2635 c.c.).
- Decreto Legislativo n. 90 del 25 maggio 2017 che recepisce la Direttiva UE 2015/849 (c.d. IV Direttiva Antiriciclaggio) relativa alla "prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo".
- Legge n.161 del 17 ottobre 2017 che introduce nuovi delitti in relazione all'immigrazione clandestina
- Legge n. 167 del 20 novembre 2017, con «Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2017» che introduce nuovi reati per «razzismo e xenofobia»
- Legge n. 179 del 30 novembre 2017, che introduce nuove "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto pubblico o privato" (il cd. Whistleblowing).
- Legge 11 gennaio 2018, n. 3, che introduce modifiche relativamente ai Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D.Lgs. n. 231/2001)
- Decreto Legislativo n. 21 del 01 marzo 2018 - Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale - che abroga l'art. 3, comma 3-bis della Legge 654/1975 (l'art. 25-terdecies) e lo sostituisce con l'art. 604 bis c.p. («razzismo e xenofobia»)
- Decreto Legislativo n. 21 del 01 marzo 2018 - Attività organizzate per il traffico illecito di rifiuti - che abroga l'art. 260 del D. Lgs. n.152/2006 e lo sostituisce con l'art. 452 quaterdecies c.p.
- La legge 9 gennaio 2019, n. 3 ("Legge Anticorruzione") che introduce, tra le altre cose, alcune significative modifiche alla disciplina della responsabilità amministrativa delle società e degli enti prevista dal d.lgs. 8 giugno 2001, n. 231. Tra le modifiche di maggior rilievo si segnalano, in particolare:
  i. l'estensione del catalogo dei reati che possono dar luogo alla responsabilità dell'ente al delitto di traffico di influenze illecite (art. 346-bis c.p.);
  ii. l'inasprimento delle sanzioni interdittive previste dall'articolo 9, comma 2 del decreto qualora sia stato commesso un reato di concussione, induzione indebita a dare o promettere utilità o corruzione. Per effetto della modifica in tali casi la durata delle sanzioni interdittive (originariamente fissata in un termine non inferiore a un anno) non potrà essere inferiore a quattro anni e superiore a sette quando il reato è

commesso da un soggetto apicale, e non inferiore a due anni e non superiore a quattro se il reato è commesso da un sottoposto.

iii. l'introduzione del beneficio della riduzione delle sanzioni interdittive per i reati di concussione, induzione indebita a dare o promettere utilità o corruzione (per un termine compreso tra 3 mesi e 2 anni) nel caso in cui l'ente si sia adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi

iv. la previsione della procedibilità d'ufficio per i reati di corruzione tra privati e di istigazione alla corruzione tra privati.

- Legge n. 39 del 3 maggio 2019, che introduce nuove disposizioni per "Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies).
- Legge n. 157 del 19 dicembre 2019 "Conversione in legge, con modificazioni del Dlgs. n. 124 del 26 ottobre 2019, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili" che introduce i reati tributari all'interno del catalogo di cui al D.Lgs. 231 (Art. 25-quinquiesdecies)".
- Decreto Legislativo n. 75 del 14 luglio 2020, che introduce nuove disposizioni per adeguare la disciplina penale italiana alla direttiva (UE) 2017/1371 del Parlamento europeo e del Consiglio, del 5 luglio 2017, in tema di lotta contro la frode che leda gli interessi finanziari dell'Unione (c.d. "direttiva PIF" – direttiva per la protezione interessi finanziari) e che introduce il reato di contrabbando all'interno del catalogo di cui al D.Lgs. 231 (Art. 25-sexiesdecies).
- Decreto Legislativo n. 184 del 08 novembre 2021 in materia di "Delitti in materia di strumenti di pagamento diversi dai contanti" che modifica l'Art. 25-octies.
- Decreto Legislativo n. 195 del 08 novembre 2021 in materia di "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio" che modifica l'Art. 25-octies
- Legge 23 Dicembre 2021, n.238, "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2019-2020" che ha introdotto alcune modifiche alle previsioni di reato richiamate dal D. Lgs. 231/2001.
- Decreto Legge n. 13 del 25 febbraio 2022, che ha introdotto alcune "Misure di contrasto alle frodi nel settore delle agevolazioni fiscali ed economiche" e conseguenti modifiche alle previsioni di reato richiamate dal D. Lgs. 231/2001:
- Legge n. 22 del 9 marzo 2022, "Disposizioni in materia di reati contro il patrimonio culturale" che ha introdotto l'Art 25 septiesdecies "Delitti contro il patrimonio culturale" e l'Art. 25 duodevicies "Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici".
- Decreto legislativo n. 19 del 02 marzo 2023, che ha recepito nel nostro ordinamento la direttiva UE 2019/2121, il cui obiettivo è "l'armonizzazione delle disposizioni concernenti le operazioni straordinarie di trasformazione e scissione transfrontaliere, nonché la modifica della disciplina delle fusioni societarie"
- Decreto Legge n. 20 del 10 marzo 2023, che ha introdotto "Disposizioni urgenti in materia di flussi di ingresso legale dei lavoratori stranieri e di prevenzione e contrasto all'immigrazione irregolare."
- Decreto legislativo n.24 del 10 marzo 2023, "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle

persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali."

- Legge n. 93 del 14 luglio 2023, che ha introdotto "Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica."
- Legge n. 137 del 09 ottobre 2023, che ha introdotto alcune "disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione" e conseguenti modifiche alle previsioni di reato richiamate dal D. Lgs. 231/2001.
- Legge n. 6 del 22 gennaio 2024, che ha per oggetto "Disposizioni sanzionatorie in materia di distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici", che ha introdotto alcune modifiche all'Art. 25-septiesdecies, del D.Lgs. 231/2001.
- Decreto Legge n. 19 del 2 marzo 2024, che ha per oggetto "Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori", che ha introdotto alcune modifiche all'Art. 25-octies, comma 1 del D.Lgs. 231/2001.
- Decreto Legislativo n. 87 del 14 giugno 2024, che ha per oggetto "Revisione del sistema sanzionatorio tributario", che ha introdotto alcune modifiche all'Art. 25-quinquesdecies, del D.Lgs. 231/2001.
- Legge 90/2024 del 28 giugno 2024, pubblicata in Gazzetta Ufficiale n. 153 del 02-07-2024, che ha per oggetto "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" che ha introdotto alcune modifiche alle previsioni di reato richiamate dal D.Lgs. 231/2001.
- Legge 112 del 08 agosto 2024, che ha per oggetto "Conversione in legge, con modificazioni, del D.L. 04 luglio 2024, n. 92, recante misure urgenti in materia penitenziaria, di giustizia civile e penale e di personale del Ministero della giustizia" e della Legge 114 del 09 agosto 2024 che ha per oggetto "Modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare" che hanno introdotto alcune modifiche all'Art. 25 del D.Lgs. 231/2001.
- Decreto legislativo del 26/09/2024 n. 141, che ha per oggetto "Disposizioni nazionali complementari al codice doganale dell'Unione e revisione del sistema sanzionatorio in materia di accise e altre imposte indirette sulla produzione e sui consumi" che hanno introdotto alcune modifiche all'Art. 25-sexiesdecies del D.Lgs. 231/2001.
- Legge 9 dicembre 2024, n. 187, che ha per oggetto "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare" che ha introdotto alcune modifiche all' Art. 25-duodecies del D.Lgs. n. 231/2001.
- Legge n. 82 del 6 giugno 2025, che ha per oggetto "Modifiche al codice penale, al codice di procedura penale e altre disposizioni per l'integrazione e l'armonizzazione della disciplina in materia di reati contro gli animali" che ha introdotto alcune modifiche all' Art. 25-undevicies del D.Lgs. n. 231/2001 - Delitti contro gli animali.
- Legge n. 80 del 9 giugno 2025, che ha per oggetto "Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario" che ha introdotto alcune modifiche all' Art. 25-sexies del D.Lgs. n. 231/2001 (Reati abuso di Mercato).
- Legge n. 132 del 23 settembre 2025, che ha per oggetto "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" che ha introdotto alcune modifiche all' Art. 25-novies del D.Lgs. n. 231/2001 - Delitti in materia di violazione del diritto d'autore -.

– Legge n. 147 del 3 ottobre 2025, che ha per oggetto “Conversione in legge, con modificazioni, del decreto legge 8 agosto 2025, n. 116, recante disposizioni urgenti per il contrasto alle attività illecite in materia di rifiuti, per la bonifica dell'area denominata Terra dei fuochi, nonché in materia di assistenza alla popolazione colpita da eventi calamitosi”, che ha introdotto alcune modifiche all’ Art. 25-undecies del D.Lgs. n. 231/2001 - Reati ambientali.

Inoltre il Decreto Legislativo n. 58 del 24 febbraio 1998 prevede, per le Società quotate, oltre al reato di abuso di informazioni privilegiate e di manipolazione del mercato, anche l’ipotesi delle corrispondenti fattispecie di illeciti amministrativi, stabilendo per essi specifiche sanzioni e l’applicazione in linea di massima dei principi enunciati dal Decreto Legislativo n. 231/2001.

La Legge n. 146 del 16 marzo 2006 ha previsto un’ulteriore estensione della responsabilità amministrativa degli enti in relazione a determinate ipotesi di reato transnazionale. In questo caso i reati presupposto non sono stati inseriti nel Decreto Legislativo n. 231/2001, ma sono contenuti nella suddetta Legge, che prevede anche le sanzioni e l’applicabilità del Decreto per i conseguenti illeciti.

Il testo attualmente in vigore del Decreto Legislativo contempla dunque le seguenti fattispecie di reato:

- art. 24 (indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello stato e di un ente pubblico);
- art. 24-bis (delitti informatici e trattamento illecito di dati);
- art. 24-ter (delitti di criminalità organizzata);
- art. 25 (concussione e corruzione);
- art. 25-bis (falsità in monete, in carte di pubblico credito e in valori di bollo);
- art. 25-bis 1 (delitti contro l’industria e il commercio);
- art. 25-ter (reati societari);
- art. 25-quater (delitti con finalità di terrorismo o di eversione dell’ordine democratico);
- art. 25-quater 1 (pratiche di mutilazione di organi genitali femminili);
- art. 25-quinquies (delitti contro la personalità individuale);
- art. 25-sexies (abusi di mercato);
- art. 25-septies (omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro);
- art. 25-octies (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio);
- art. 25-novies (delitti in materia di violazione del diritto d’autore);
- art. 25-decies (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria);
- art. 25-undecies (reati ambientali);
- art. 25-duodecies (impiego di cittadini di paesi terzi il cui soggiorno è irregolare);
- art. 25-terdecies (Razzismo e xenofobia).
- art. 25-quaterdecies (Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati).

- art. 25-quinquiesdecies (Reati tributari)
- art. 25-sexiesdecies (reato di contrabbando)
- art. 25-septiesdecies (delitti contro il patrimonio culturale)
- Art. 25-duodevicies (Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici)

Ad esse si aggiungono altresì i seguenti reati transnazionali, di cui all'art. 10 della Legge 146/2006, in quanto ai conseguenti illeciti amministrativi previsti da detto articolo si applicano le disposizioni di cui al D. Lgs. n. 231/2001.

- art. 416 c.p. associazione per delinquere;
- art. 416-bis c.p. associazione di tipo mafioso;
- art. 291-quater T.U. D.P.R. 43/73 (materia doganale) associazione per delinquere finalizzata al contrabbando di tabacchi esteri;
- art. 74 del T.U. D.P.R. 309/90 associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope;
- art. 12 commi 3, 3bis, 3ter e 5 del T.U. di cui al D.Lgs. n.286/98 disposizioni contro le immigrazioni clandestine;
- art. 377-bis c.p. induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria;
- art. 378 c.p. favoreggiamento personale.

Riprendendo l'esame della responsabilità degli enti, si sottolinea come, per il meccanismo di accertamento di tale tipo di responsabilità, essa venga definita "amministrativa" in omaggio al principio costituzionale della personalità della responsabilità penale, anche se il "modus operandi" la avvicina in più punti ad una responsabilità penale sia per il tipo di processo, sia per le sanzioni comminate, sia ancora per l'autorità giudicante e inquirente (penale) ed infine per la possibilità di adottare misure cautelari.

Il processo a cui è fatto riferimento si articolerà quindi in due autonomi giudizi: uno nei confronti del collaboratore indagato ed un altro nei confronti dell'ente.

Sono previste sanzioni (ex art. 9 e 10) pecuniarie ed eventualmente, per i casi più gravi, l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni funzionali alla commissione dell'illecito, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni o sussidi, il divieto di pubblicizzare beni o servizi, la confisca del prezzo o del profitto del reato, e la pubblicazione della sentenza.

Particolare rilevanza assumono le "sanzioni interdittive", che si applicano in relazione ai reati per i quali sono espressamente previste e quando ricorrono le condizioni indicate dall'art. 13: la loro gravità deriva anche dalla comminabilità in sede cautelare.

Le sanzioni possono essere evitate ove l'ente adotti modelli di comportamento (procedure di autocontrollo) idonei a prevenire i reati.

Il Modello deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire e ad eliminare tempestivamente situazioni di rischio.

Inoltre, l'efficace attuazione del Modello richiede una verifica periodica e l'eventuale modifica dello stesso quando siano scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività.

L'Ente non risponde se prova che:

1. in caso di reato presupposto commesso dai cosiddetti "soggetti apicali":
    a. l'organo dirigente ha adottato (e provato di avere efficacemente attuato) prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi ed ha affidato ad un proprio organismo, dotato di autonomi poteri dì iniziativa e di controllo, l'onere di vigilare e di curare il loro aggiornamento;
    b. le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione ovvero non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di controllo di cui al precedente punto a.
2. in caso di reato presupposto commesso da persone sottoposte alla direzione e alla vigilanza di un apicale:
    a. non vi è stata inosservanza degli obblighi di direzione o vigilanza. Tale inosservanza è in ogni caso esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Si ricorda che il Decreto, all'articolo 6, pone a carico dell'ente l'onere di provare l'avvenuta adozione delle misure preventive solo nel caso in cui l'autore del reato sia un soggetto "apicale" come sopra definito ("inversione dell'onere della prova").

Sulla base dell'interpretazione letterale della norma, si ritiene invece che, nel caso in cui l'autore del reato sia sottoposto all'altrui direzione o vigilanza, l'onere probatorio, relativo alla mancata adozione delle misure preventive, spetti al Pubblico Ministero.

Si ricorda nuovamente che ai fini del Decreto si considera soggetto in posizione apicale colui che riveste funzioni di rappresentanza dell'ente, di amministrazione o direzione dell'ente ovvero di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (ad esempio institori), nonché coloro che esercitano, anche di fatto, la gestione e il controllo dello stesso.

2.2 Il Decreto Legislativo 81 del 9 aprile 2008

Il legislatore del D.Lgs. n. 81/2001, tenuto conto della particolarità del contesto di riferimento, all'art. 30 ha inteso individuare più specificamente gli obiettivi ed i contenuti, anche ulteriori rispetto a quelli indicati negli art. 6 e 7 del D.Lgs. n. 231/2001, che devono caratterizzare i Modelli organizzativi perché questi possano essere giudicati idonei ed efficacemente adottati, con conseguente possibilità per l'Ente, in tali ipotesi, di beneficiare dell'efficacia esimente ad essi riconosciuta.

In particolare, il Modello organizzativo dovrà essere adottato ed efficacemente attuato, in modo tale da assicurare 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.

Proseguendo, l'art. 30 richiede espressamente che il modello organizzativo preveda:

- idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui sopra. Tale previsione, da un lato, facilita l'attività investigativa documentale della polizia giudiziaria finalizzata all'accertamento della responsabilità amministrativa dell'ente; dall'altro, offre all'ente la possibilità di "opporre" una preliminare difesa a dimostrazione della assenza di responsabilità;
- per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche ed 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;
- 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.

  In sede giurisprudenziale, il Tribunale di Trani, con la sentenza in data 29.10.2009, ha statuito la necessità che l'impianto del Modello, allorquando non siano coinvolti soggetti dipendenti dell'ente, preveda comunque l'adozione di cautele e regole per evitare che dipendenti di enti terzi possano subire lesioni o perdere la vita per infrazioni commesse dai loro datori di lavoro nell'esecuzione delle attività lavorative loro assegnate. In particolare, è stato chiarito che il controllo dei rischi non può esaurirsi nell'ambito della struttura organizzativa ed aziendale della società in questione, ma deve essere esteso anche all'osservanza delle medesime regole da parte dei soggetti che con quest'ultima entrano, direttamente o indirettamente, in rapporti lavorativi.

L'adozione e l'efficace attuazione del Modello di verifica e controllo assume, inoltre, particolare rilievo in termini di riconoscimento dell'avvenuto adempimento dell'obbligo di vigilanza nei confronti del delegato da parte del Datore di Lavoro delegante, secondo quanto previsto dall'art. 16, comma 3, del D.Lgs. n. 81/2008. Quest'ultimo stabilisce infatti che tale obbligo di vigilanza si intende assolto in caso di adozione ed efficace attuazione del Modello di verifica e controllo di cui all'articolo 30, comma 4.

In punto di idoneità del Modello, il comma 5 dell'articolo in esame introduce una presunzione di legge secondo cui si considera conforme alle prescrizioni sopra riportate il Modello organizzativo adottato dall'ente definito 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 per le parti corrispondenti.

In merito, inoltre, è previsto, ai sensi del combinato disposto dell'art. 6 e dell'art. 30, comma 5-bis del D.Lgs. n. 81/2008, che la Commissione consultiva permanente per la salute e sicurezza sul lavoro può indicare Modelli di organizzazione e gestione aziendale, nonché elaborare procedure semplificate per l'adozione e l'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.

Rilevante ai fini che qui interessano è anche la disposizione contenuta all‟art. 51, comma 3- bis secondo cui gli organismi paritetici di cui all'art. 1, comma 2, lettera e), su richiesta delle imprese, possono rilasciare l'asseverazione dell'adozione e dell'efficace attuazione dei Modelli di organizzazione e gestione della sicurezza di cui all'articolo 30.

Si ricorda inoltre che è stato statuito in sede giurisprudenziale (cfr. Tribunale di Trani, sentenza in data 26 ottobre 2009), che i documenti di valutazione dei rischi redatti ai sensi degli artt. 26 e 28 del D.Lgs. n. 81/2008:

- non sono equiparabili al Modello organizzativo e gestionale di cui al D.Lgs. n. 231/2001;
- non assumono valenza nella direzione di assicurare l'‟efficacia esimente" di cui agli artt. 6 e 7.

In merito, occorre rilevare che il sistema introdotto dal D.Lgs. n. 231/2001 impone agli enti di adottare un Modello organizzativo diverso e ulteriore rispetto a quello previsto dalla normativa antinfortunistica, onde evitare in tal modo la responsabilità amministrativa.

Non a caso, mentre i documenti di valutazione dei rischi nel contesto normativo di cui al D.Lgs. n. 81/2008 sono disciplinati dagli artt. 26 e 28, il Modello di organizzazione e gestione di cui al D.Lgs. n. 231/2001 è contemplato dall'art. 30 del citato D.Lgs. n. 81/2008, segnando così una distinzione non solo nominale ma anche funzionale.

2.3 Ulteriori fonti

Ad integrazione dei punti precedenti, sono state impiegate anche le seguenti ulteriori fonti normative, per quanto di interesse 231:

- D.P.R. 62/2013, "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165";
- Circolare n. 83607/2012 del Comando Generale della Guardia di Finanza - III Reparto Operazioni - Ufficio Tutela Economia e Sicurezza: "Attività della Guardia di Finanza a tutela del mercato dei capitali - Parte IV: Disposizioni comuni".

Alle suddette fonti normative si è fatto riferimento, nel presente Modello, per la redazione dei protocolli afferenti nonché per la valutazione dei rischi all'interno della fase di Risk Assessment.

Con riferimento alla Circolare della Guardia di Finanza, essa è stata impiegata quale elemento per la definizione dell'Organismo di Vigilanza.

2.4 Il Modello di organizzazione gestione e controllo

Come detto, il Decreto ha introdotto la responsabilità amministrativa "penale" degli enti, i quali possono essere ritenuti responsabili, e di conseguenza sanzionati con pene patrimoniali e interdittive, in relazione alla commissione di un "reato presupposto", nell'interesse o vantaggio degli enti stessi, da parte degli amministratori, degli altri soggetti apicali o dei collaboratori.

Gli enti possono adottare un Modello 231 idoneo a prevenire i reati stessi.

Tra i reati attualmente più rilevanti, in quanto commissibili dalla maggioranza degli enti, al fine di configurarne la responsabilità "penale", possono essere ricomprese le seguenti categorie:

- reati contro la Pubblica Amministrazione,
- reati societari,
- reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro,
- reati ambientali.

L'accertamento della responsabilità dell'ente è attribuito al giudice penale mediante:

- la verifica della sussistenza del reato,

e

- il sindacato di idoneità sul modello organizzativo adottato.

Il Modello contiene o rinvia a un complesso di principi, regole, protocolli, documenti organizzativi (organigramma, mansionari, etc.) funzionale alla prevenzione dei reati previsti dal Decreto. Inoltre esso comprende una clausola risolutiva espressa da applicare ai fornitori contrattualizzati.

Il Modello della FORMARE S.r.l. (di seguito anche la "Società") è emanazione dell'Organo di Amministrazione, che provvede ad approvarlo.

Il compito di attuare il Modello è dell'Organo di Amministrazione mediante l'emanazione delle opportune disposizioni interne.

Sono destinatari del Modello tutti coloro che operano per il conseguimento dello scopo e degli obiettivi della Società, e pertanto in generale gli esponenti della stessa, i componenti l'Organismo di Vigilanza, i dipendenti, i collaboratori anche parasubordinati, i consulenti esterni.

Per esponente si intendono, come di volta in volta in carica, l'Organo di Amministrazione ed l'Organo di Controllo se nominato, nonché i membri degli altri Organi Sociali dell'ente eventualmente istituiti. Si intende, inoltre, qualsiasi altro soggetto in posizione apicale che rivesta funzioni di rappresentanza, amministrazione o direzione, gestione, controllo dell'ente, ai sensi del Decreto.

L'adozione del presente Modello Organizzativo è comunicata a tutte le risorse operanti per la struttura al momento della sua delibera di approvazione.

Il Modello consta di una Parte Generale e di una Parte Speciale: la prima illustra il contesto normativo di riferimento, gli obiettivi, le linee della struttura societaria e le modalità di implementazione del Modello stesso, mentre la seconda è relativa alle tipologie di reato specificamente sanzionate dal Decreto. In particolare, il Modello Parte Speciale esamina le fattispecie di reato presupposto, identifica le aree in cui sussiste un rischio di commissione di reato e valuta i sistemi di controllo di tali attività. Si sostanzia nella mappa dei rischi attività sensibili "231".

Più specificamente, la Parte Speciale consiste nella Mappatura dei rischi, in cui sono state identificate delle attività che, esclusivamente in relazione ai loro specifici contenuti, potrebbero essere esposte (o maggiormente esposte) al rischio di commissione dei reati contemplati dal Decreto.

Per la sua elaborazione, si è proceduto - previa l'opportuna ricognizione - ad associare ai processi organizzativi interni (nel cui svolgimento, in via teorica, potrebbero integrarsi gli estremi di reato di cui alla normativa in esame) le varie fattispecie di reato considerate dal Decreto.

Le aree di rischio individuate sono da intendersi come un complesso in evoluzione, da adeguarsi periodicamente in relazione a modifiche normative e/o a variazioni interne.

Le regole di condotta contenute nel presente Modello si integrano con quelle del **Codice Etico** adottato dalla Società nonché con quelle contenute nei Sistemi di Gestione certificati dei quali la Società si è dotata (di cui in seguito).

2.5 Lo scopo del Modello

Scopo del Modello è quello di fornire indicazioni sui contenuti del Decreto e sul particolare tipo di responsabilità amministrativa degli enti che esso introduce nel nostro ordinamento per i reati commessi, nel loro interesse o vantaggio, dai propri esponenti o dipendenti.

È inoltre volto ad indirizzare le attività interne affinché siano in linea con lo stesso e a vigilare sul suo funzionamento e sulla sua osservanza.

In particolare il Modello ha la finalità di:

- generare, in tutti coloro che operano in nome e per conto dell'ente, la consapevolezza di poter incorrere, in caso di violazione delle norme richiamate dal Decreto, in un illecito, passibile di sanzioni nei propri confronti e nei riguardi dell'ente (se questo ha tratto vantaggio dalla commissione del reato, o comunque se quest'ultimo è stato commesso nel suo interesse);
- chiarire che i comportamenti illeciti sono condannati dalla Società in quanto contrari sia alle disposizioni di legge sia ai principi cui essa intende attenersi nell'espletamento della propria missione;
- fissare e rendere noti tali principi, indicandoli nel Modello e nel Codice Etico adottati;
- implementare, in particolare attraverso l'Organismo di Vigilanza, azioni di monitoraggio e controllo interno, indirizzate soprattutto agli ambiti gestionali più esposti in relazione al Decreto, nonché la formazione dei collaboratori al corretto svolgimento dei loro compiti, al fine di prevenire e contrastare la commissione dei reati stessi;
- prevedere delle sanzioni a carico dei destinatari del presente Modello che lo abbiano violato, ovvero abbiano commesso un illecito sanzionabile ai sensi del Decreto.

2.6 Le modalità di redazione del Modello

Il Modello della Società è stato predisposto sulla base delle norme contenute nel Decreto, sulla base della versione aggiornata delle linee guida elaborate da Confindustria, nonché sulla base di quanto previsto dal Decreto Legislativo 9 aprile 2008, n. 81 e sue integrazioni e/o successive modificazioni.

Ciò in quanto, ai sensi del Decreto, i Modelli possono essere sviluppati sulla base dei codici di comportamento redatti dalle associazioni di categoria rappresentative degli enti, comunicate al Ministero di Giustizia il quale, se del caso, può formulare osservazioni. Posto dunque che la Direzione Generale Giustizia Penale si è espressa positivamente rispetto alle Linee Guida formulate da Confindustria, il presente Modello è stato elaborato in linea con le indicazioni ivi contenute, quali risultanti dopo la modifica di giugno 2021.

Non sono state prese in considerazione ulteriori linee guida predisposte da altre associazioni di categoria.

In attuazione di quanto previsto all'art. 6, comma 3, del Decreto, Confindustria ha definito le proprie Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo nelle quali vengono fornite alle imprese associate indicazioni metodologiche su come individuare le aree di rischio e strutturare il Modello.

Tali Linee Guida suggeriscono alle società di utilizzare i processi di risk assessment e risk management e prevedono le seguenti fasi per la definizione del modello:

1. l'identificazione dei rischi;
2. la predisposizione e/o l'implementazione di un sistema di controllo idoneo a prevenire il rischio di cui sopra attraverso l'adozione di specifici protocolli.

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

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

   Dette componenti devono essere informate ai principi di:

   - verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
   - applicazione del principio di separazione delle funzioni;
   - documentazione dei controlli;
   - previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal modello;
   - autonomia, indipendenza, professionalità e continuità d'azione dell'Organismo di Vigilanza;
3. individuazione dei criteri per la scelta dell'organismo di controllo (o "Organismo di Vigilanza") e previsione di specifici flussi informativi da e per l'organismo di controllo;

4. possibilità, nei gruppi societari, di adottare soluzioni organizzative che accentrino presso la capogruppo le funzioni previste dal Decreto, purché presso ciascuna società controllata sia istituito un organismo di controllo che possa avvalersi delle risorse, professionali e finanziarie, allocate presso l'analogo organismo della capogruppo sulla base di un rapporto contrattuale con la stessa. Tale disponibilità dovrà permettere a ciascun organismo, costituito presso le società controllate, di svolgere in concreto le attività di controllo previste, mediante risorse qualificate come professionisti esterni.

3 IL PROFILO DELLA SOCIETÀ

3.1 La storia e la Mission

Fondata nel 1985 ad opera della - FEDERLAZIO Associazione delle Piccole e Medie Imprese del Lazio - con lo scopo di soddisfare i fabbisogni formativi del management delle piccole e medie imprese associate. Formare Srl è un piccolo ente di formazione senza fini di lucro che ha mantenuto negli anni l'obiettivo principale di:

- Dare una risposta seria e professionale ai fabbisogni formativi delle imprese
- Incentivare la cultura e la conoscenza del life long learning e dell'apprendimento continuo nelle piccole e medie imprese
- Valorizzare il capitale umano

In virtù della mission espressa, gli obiettivi da perseguire sono stabiliti in:

- Proposte formative "su misura " del cliente e dell'utente
- Proposte innovative e compatibili con le professionalità richieste dal mercato
- Ricerca e applicazione di metodologie didattiche attive innovative e compatibili con lo sviluppo delle nuove tecnologie
- Tempestività del servizio
- Flessibilità organizzativa
- Monitoraggio della Customer Satisfaction

Formare Srl punta soprattutto sulla preparazione manageriale degli imprenditori, dei dirigenti e quadri aziendali, rivolgendosi a persone già inserite nel mondo del lavoro che vogliono investire sulla loro formazione e preparazione.

La Società favorisce l'ingresso dei giovani nel Mercato del lavoro attraverso:

a) Matching domanda-offerta
b) tirocini formativi e di inserimento al lavoro
c) Formazione dei giovani neo-assunti

3.2 I Servizi offerti

Formare Srl punta soprattutto sulla preparazione manageriale degli imprenditori, dei dirigenti e quadri e vanta una lunga esperienza nella Progettazione, Consulenza ed Assistenza alle imprese per lo sviluppo di interventi formativi.

Per l'erogazione dei servizi Formare Srl opera con le aziende nella Formazione finanziata, lavorando con i principali Fondi Interprofessionali, con il Fondo Sociale e Fondi Comunitari, Fondi INAIL e SICUREZZA.

Formare Srl è accreditata presso la Regione Lazio per:

- la Formazione Continua e Superiore
- Formazione in Apprendistato Professionalizzante
- Sportello Tirocini

La società organizza ed eroga formazione rivolta a tutte le tipologie di utenza, per l'aggiornamento, il perfezionamento, la specializzazione, la riqualificazione e l'acquisizione di specifiche competenze professionali, offrendo formazione a Catalogo e Corsi aziendali ad hoc.

3.3 Le Sedi

La Sede principale di Formare Srl è a Roma in Viale Libano n.62 (Eur) ed opera sul territorio Nazionale e Comunitario attraverso Reti con partner qualificati e consolidati.

Formare Srl opera inoltre in tutta la Regione Lazio presso le sedi provinciali della Federlazio, in:

- Frosinone Via Marco Tullio Cicerone 152
- Latina Piazza Mercato 11
- Rieti Via Sani zi 2
- Viterbo Via Sacchi 18

Dove dispone di aule didattiche che possono ospitare da 20 a 40 ospiti, attrezzate con PC, lavagna a fogli mobili, lavagna luminosa, videoproiettore, Tv e Connessione Internet.

4 IL SISTEMA DI CORPORATE GOVERNANCE DELLA SOCIETÀ

La Società adotta un sistema di Corporate Governance conforme al modello tradizionale nel rispetto da quanto delineato dalla legge e dalle specificità riportate nello statuto.

Per quanto all'Organo di controllo la Società, non sussistendo i requisiti minimi previsti dal 3 comma dell'articolo 2477 del c.c., ha ritenuto di non procedere alla nomina né del Collegio Sindacale né del revisore legale dei conti, così come richiamato dalla norma sopra indicata.

Per quanto riguarda il funzionamento della Società nell'ambito del modello tradizionale si rimanda integralmente alle norme del codice civile, e quelle contrattuali dello statuto, che costituisce parte integrante del presente modello.

4.1 Decisioni dei soci

I soci decidono sugli argomenti che uno o più amministratori o tanti soci che rappresentano almeno un tetto del capitale sociale sottopongono alla loro approvazione nonché sulle materie riservate alla loro competenza dalla legge.

Ogni socio ha diritto di partecipare alle decisioni sopra indicate ed il suo voto vale in misura proporzionale alla sua partecipazione fermo restando che il socio moroso non può partecipare alle decisioni dei soci.

Le decisioni dei soci possono adottate mediante deliberazione assembleare ai sensi dell'art. 2479 bis c.c., ovvero mediante consultazione scritta o sulla base del consenso espresso per iscritto.

Le decisioni non assembleari sono prese con il voto favorevole dei soci di una maggioranza che rappresenti almeno la metà del capitale sociale. Devono essere adottate mediante deliberazione assembleare ai sensi dell'art. 2479 bis c.c. le deliberazioni di cui ai nn. 4 e 5 dell'art. 2479 c.c. ovvero quando lo richiedano uno o più amministratori o un numero di soci che rappresentino almeno un terzo del capitale sociale.

Nel caso di decisione mediante consultazione scritta, il testo della decisione da adottare, dal quale risulti con chiarezza il relativo argomento, è predisposto da uno o più amministratori o da tanti soci che rappresentino almeno un terzo del capitale sociale. Esso dovrà indicare il termine entro il quale tale decisione dovrà pervenire presso la sede sociale e di ciò dovranno essere informati tutti i soci, l'organo amministrativo e, se nominato, l'organo preposto al controllo dei conti.

La decisione si perfeziona validamente quando tutti i soci siano stati interpellati ed almeno la maggioranza prescritta abbia espresso e comunicato alla società il proprio consenso alla decisione proposta.

Il termine entro il quale la decisione dovrà pervenire presso la sede sociale non potrà comunque essere inferiore ad 8 (otto) giorni dal momento della spedizione della suddetta comunicazione.

Le decisioni potranno essere comunicate con qualsiasi i mezzo purché dai documenti sottoscritti risulti con chiarezza la provenienza, l'argomento oggetto della decisione ed il consenso alla stessa.

Nel caso in cui la decisione sia adottata mediante consenso espresso per iscritto ciascun socio presta il proprio consenso senza che via stata formale interpellanza. Il consenso viene manifestato da ciascun socio mediante sottoscrizione di un documento dal quale risulti con chiarezza l'argomento oggetto della decisione. La decisione si perfeziona validamente quando almeno la maggioranza prescritta abbia espresso e comunicato alla società il proprio consenso su un testo di decisione sostanzialmente identico.

Sono in ogni caso riservate ai soci le decisioni riguardanti:

a) l'approvazione del bilancio e la distribuzione degli utili;
b) la nomina degli amministratori;
c) la nomina, nei casi previsti dall'articolo 2477 c.c. dei sindaci e del Presidente del collegio sindacale o del revisore;

Sono invece riservate alla competenza dell'assemblea dei soci;

a) le modificazioni dell'atto costitutivo;
b) le decisioni di compiere operazioni che comportino una sostanziale modifica dell'oggetto sociale determinato nell'atto costitutivo o una rilevante modificazione dei diritti dei soci.

Le decisioni assunte ai sensi del presente articolo devono essere trascritte senza indugio nel libro delle decisioni dei soci a cura dell'organo amministrativo.

4.2 Assemblee

Le assemblee dei soci di cui all'art. 2479 bis del c.c. sono tenute di regola, presso la sede sociale, salvo diversa determinazione dell'organo amministrativo che può fissare un luogo diverso, purché sito nel territorio dello Stato.

L'assemblea deve essere convocata almeno una volta all'anno, entro centoventi giorni dalla chiusura dell'esercizio sociale o entro centottanta giorni se ricorrono le condizioni previste dal secondo comma dell'articolo 2364 c.c.

L'assemblea è convocata e delibera, oltre che nei casi e per gli oggetti previsti dalla legge e dal presente statuto, ogni qualvolta l'organo amministrativo o tanti soci che rappresentino almeno 1/3 (un terzo) dell'Assemblea si costituisce e delibera con la maggioranza di legge e di statuto.

Possono intervenire all'assemblea i soggetti regolarmente iscritti nel libro soci.

Ogni socio che abbia il diritto dii intervenire all'assemblea può farsi rappresentare ai sensi dell'art.2479 bis c.c..

La rappresentanza non può essere conferita né a membri dell'organo amministrativo o di controllo né a dipendenti della società né alle società da essa controllate o ai membri degli organi amministrativi o di controllo o ai dipendenti di queste.

Gli enti e le società legalmente costituiti possono intervenite all'assemblea a mezzo di persona designata mediante delega scritta.

Spetta al Presidente dell'assemblea di constatare la regolarità delle deleghe e, in genere, il diritto di intervento all'assemblea. Quando tale constatazione è avvenuta la validità della costituzione dell'assemblea non potrà essere infirmata per il fatto che alcuni degli intervenuti abbandonino l'adunanza.

La presidenza dell'assemblea secondo i sistemi di amministrazione compete:

- all'Amministratore Unico;
- al Presidente dei Consiglio di Amministrazione e in caso di assenza od impedimento del Presidente, nell'ordine: al Vice Presidente ed all'Amministratore Delegato se nominati.

Qualora né gli uni né gli altri possano o vogliano esercitare tale funzione, gli intervenuti designano, a maggioranza assoluta delle partecipazioni rappresentate, il Presidente tra i presenti.

L'assemblea nomina un segretario, anche non socio, e se lo crede opportuno, due scrutatori anche estranei.

Le deliberazioni dell'assemblea devono risultare dal verbale firmato dal Presidente, dal segretario ed eventualmente dagli scrutatori.

Nei casi di legge e, inoltre, quando il Presidente dell'assemblea lo ritenga opportuno, il verbale viene redatto da un notaio.

L'assemblea è convocata, a cura dell'organo amministrativo mediante avviso da spedirsi almeno otto giorni prima di quello fissato per l'adunanza. L'avviso dovrà contenere l'indicazione del giorno, dell'ora e del luogo della riunione nonché l'elenco degli argomenti da trattare.

L'avviso può essere spedito, al domicilio indicato nel libro soci, oltre che per raccomandata, a mezzo di telegramma, fax, telex, posta elettronica ed in qualunque altro modo che sia idoneo ad assicurare la tempestiva informazione.

Sono valide le assemblee totalitarie di cui all'ultimo comma dell'art. 2479 bis.

Il voto di ciascun socio vale in proporzione alla sua quota di partecipazione. L'assemblea è validamente costituita quando sia rappresentata almeno la metà del capitale sociale.

L'assemblea decide sulle materie di ordinaria gestione con il voto favorevole di tanti soci che rappresentino la maggioranza assoluta delle partecipazioni sociali intervenute.

L'assemblea decide sulla materie dì cui ai numeri 4 e 5 dell'art. 2479 con il voto favorevole di una maggioranza che rappresenti almeno la metà del capitale sociale.

Restano comunque salve le altre disposizioni di legge o del presente statuto che, per particolari decisioni, richiedano specifiche maggioranze.

Le decisioni sono prese per alzata di mano a meno che la maggioranza richieda l'appello nominale.

La nomina alle cariche sociali può avvenire per acclamazione se nessun socio vi si oppone.

4.3 Amministrazione

La Società può essere amministrata:

- da un Amministratore Unico;
- da un Consiglio di Amministrazione composto da 2 (due) a 5 (cinque) membri.

I soci con propria decisione scelgono il sistema di amministrazione e, nel caso di Consiglio, fissano il numero dei membri.

Il Consiglio di Amministrazione opera con il metodo collegiale a meno che, all'atto della nomina, non venga previsto che Io stesso operi con metodo disgiuntivo o congiuntivo.

I componenti dell'organo amministrativo:

a) possono essere anche non soci;

b) durano in carica, secondo quanto stabilito all'atto della nomina, a tempo indeterminato fino a revoca ovvero per il periodo di volta in volta determinato;

c) sono tenuti al divieto di cui all'art. 2390 c.c..

4.4 Consiglio di Amministrazione

Quando la società è amministrata da un Consiglio di Amministrazione, il funzionamento dello stesso è cosi regolato:

A - Presidenza.

Il Consiglio elegge fra i suoi membri il Presidente se questi non è nominato dall'assemblea; può eleggere un Vice Presidente che sostituisca il Presidente nei casi di assenza o impedimento.

B - Riunioni.

Il Consiglio si riunisce nel luogo indicato nell'avviso di convocazione (nella sede sociale o altrove purché in Italia) tutte le volte che il Presidente o chi ne fa le veci lo giudichi necessario, o quando ne sia fatta richiesta dalla maggioranza degli amministratori in carica, oppure da almeno due sindaci o dal revisore.

Di regola la convocazione è fatta almeno cinque giorni liberi prima della riunione. Nei casi di urgenza il termine può essere più breve ma non inferiore ad un giorno.

Le riunioni di Consiglio sono presiedute dal Presidente, in sua assenza, dal Vice Presidente, qualora sia stato nominato, o, in mancanza anche di quest'ultimo dal consigliere designato dal consiglio stesso.

Il Consiglio di Amministrazione può riunirsi anche in video-conferenza o teleconferenza purché ricorrano le seguenti condizioni:

- il Presidente del Consiglio di Amministrazione deve poter accertare l'identità degli intervenuti, regolare lo svolgimento della riunione, constatare e proclamare i risultati della riunione;
- il Presidente del Consiglio di Amministrazione ed il soggetto deputato alla verbalizzazione devono essere presenti nello stesso luogo in modo da provvedere alla redazione ed alla sottoscrizione del verbale;
- il Presidente del Consiglio di Amministrazione ed il soggetto deputato alla verbalizzazione devono poter percepire adeguatamente gli eventi oggetto di discussione e verbalizzazione
- gli intervenuti devono poter partecipare alla discussione in tempo reale e votare in simultanea sugli argomenti posti all'ordine del giorno e, ove necessario, prendere visione, ricevere ed inviare documenti.

La riunione del Consiglio di Amministrazione in video conferenza o teleconferenza si intenderà tenuta nel luogo in cui si trovano il Presidente ed il soggetto addetto alla verbalizzazione e si considereranno intervenuti i soggetti la cui identità sia stata accertata dal Presidente del Consiglio di Amministrazione.

C - Decisioni.

Per la validità delle decisioni del Consiglio è necessaria la presenza della maggioranza degli amministratori in carica.

Le decisioni si prendono a maggioranza assoluta degli intervenuti, in caso di parità prevale il voto di chi presiede.

Le decisioni del Consiglio di Amministrazione possono essere adottate mediante consultazione scritta o mediante consenso espresso per iscritto. In tal caso la decisione viene adottata sulla base del

consenso della maggioranza assoluta degli amministratori, sempreché dai documenti sottoscritti emergano con chiarezza l'argomento oggetto della decisione ed il consenso alla stessa.

D - Verbalizzazioni

Le decisioni del Consiglio di Amministrazione e del Comitato Esecutivo, se nominato ai sensi della successiva lettera "E", devono risultare da verbali che trascritti su apposito libro tenuto a norma di legge, vengono firmati da chi presiede e dal segretario nominato di volta in volta anche tra estranei al consiglio.

E - Delega dei poteri.

Nei limiti e con le modalità previste dall'articolo 2381 c.c. e dalle altre leggi vigenti, il Consiglio di Amministrazione può delegare le proprie attribuzioni a un Comitato Esecutivo composto di alcuni dei suoi membri o ad uno o più Amministratori Delegati, determinando i limiti della delega.

Le cariche di Presidente (o di Vice Presidente) e di Amministratore Delegato sono cumulabili.

4.5 Poteri dell'Organo Amministrativo

Qualunque sia il sistema di amministrazione della società, l'organo amministrativo è investito dei poteri attribuiti espressamente in sede di nomina ovvero dall'atto costitutivo.

Nel caso che la società sia amministrata da un Consiglio di Amministrazione all'atto della nomina potrà essere indicato se l'amministrazione viene conferita agli amministratori in modo disgiuntivo o congiuntivo e con le modalità di azione congiunta o disgiunta.

In mancanza di espressa determinazione di poteri all'organo amministrativo spettano i poteri di ordinaria e straordinaria amministrazione fatta eccezione per quanto è riservato dalla legge o dall'atto costitutivo alle decisioni dei soci.

Dovrà essere comunque adottata con metodo collegiale la redazione del bilancio e dei progetti di fusione e di scissione nonché le decisioni di aumento del capitale ai sensi dell'art.2481 del cc.

4.6 Rappresentanza della Società

La rappresentanza della società compete all'Amministratore Unico od al Presidente del Consiglio di Amministrazione senza limitazioni, ed ai membri del Consiglio di Amministrazione fomiti dei poteri delegati nei limiti della delega; nonché a ciascuno degli amministratori in caso di amministrazione disgiuntiva o a tutti gli amministratori congiuntamente in caso di amministrazione congiuntiva.

L'organo amministrativo può nominare direttori generali, amministrativi e tecnici, nonché procuratori per singoli affari o per categorie di affari.

4.7 Direttori

Il Direttore della Società è il Direttore Generale dell'unico socio FEDERLAZIO ASSOCIAZIONE PICCOLE E MEDIE IMPRESE DEL LAZIO".

Il Direttore è preposto alla direzione della società, coordina e sovrintende alle attività degli uffici, coadiuva il Presidente ovvero l'Amministratore Unico, partecipa all'assemblea con voto consultivo, svolge le funzioni di segretario, è il capo del personale ed in tale veste gli sono affidate le assunzioni ed i licenziamenti del personale dipendente.

4.8 Compensi degli Amministratori

Ai componenti dell'organo amministrativo potrà spettare un compenso annuo, da determinarsi dall'assemblea, in misura fissa e/o in misura variabile, da calcolarsi percentualmente sugli utili di bilancio al lordo delle imposte ed indennità di fine rapporto, oltre al rimborso delle spese sostenute per l'esercizio ed a causa delle loro funzioni.

4.9 Controllo contabile e sulla gestione

Qualora sia obbligatorio per legge l'assemblea nomina un Collegio Sindacale composto di tre o cinque membri effettivi e due supplenti, soci o non soci che ha anche funzioni di controllo contabile. Le competenze ed i poteri di tale organo verranno stabilite all'atto di nomina. Il Collegio Sindacale vigila sull'osservanza della legge e dello Statuto. Per il suo funzionamento e la retribuzione dei Sindaci valgono le norme di legge. Qualora la nomina del Collegio Sindacale non sia obbligatoria l'Assemblea potrà comunque procedere alla nomina del Collegio Sindacale composto di tre membri effettivi e due supplenti ovvero di un Revisore iscritto nel Registro istituto presso il Ministero della Giustizia, cui sarà devoluto il controllo legale e contabile della Società.

4.10 Esercizio sociale - Bilancio

L'esercizio si chiude ai 31 (trentuno) dicembre di ogni anno. Alla fine di ogni esercizio l'Organo amministrativo provvede in conformità alle prescrizioni di legge, alla formazione del bilancio sociale.

4.11 Utili

La decisione dei soci che approva il bilancio decide sulla distribuzione degli utili. Non può farsi luogo a distribuzione di utili se si verifica una perdita del capitale sociale fino a che il capitale sia stato reintegrato o ridotto in misura corrispondente.

4.12 Soggetti in posizione apicale

Come in precedenza indicato, il Decreto richiede di individuare i soggetti in posizione apicale. Fermo restando il dettato normativo di cui all'art. 5 del Decreto e la relativa prassi applicativa, i criteri per individuare tali soggetti possono essere così sintetizzati:

- collocazione gerarchica al vertice della Società o al primo livello di riporto;
- assegnazione di poteri di spesa e di deleghe che consentano di svolgere talune attività, anche verso l'esterno, con un certo margine di autonomia.

I predetti requisiti devono sussistere congiuntamente e non sono alternativi. È pertanto possibile identificare i soggetti apicali avvalendosi dell'organigramma aziendale.

Alla luce dei criteri sopra esposti, allo stato non risultano altri soggetti apicali della Società, oltre agli Organi sopra elencati.

5 I SISTEMI MANAGERIALI RILEVANTI

5.1 Il sistema organizzativo

Il sistema organizzativo è coerente rispetto ai seguenti principi ispiratori:

- adeguata formalizzazione;
- chiarezza delle linee di dipendenza gerarchica e funzionale;
- pubblicità dei poteri attribuiti, sia all'interno sia all'esterno della Società, per garantirne la conoscibilità;
- chiarezza sul conferimento dei poteri e sulla conseguente allocazione delle responsabilità, così come sulle responsabilità organizzative interne.

Nel suo complesso, il sistema organizzativo consta di:

1. Struttura organizzativa. È rispecchiata nell'organigramma aziendale, che indica l'articolazione delle funzioni interne ed i relativi responsabili;
2. Sistema delle deleghe in materia di sicurezza;
3. Procedure e Istruzioni operative, che definiscono le modalità operative per lo svolgimento delle diverse attività.

I documenti di cui ai punti precedenti non vengono allegati al presente Modello a causa della loro analiticità e della possibile frequenza di modificazione, ma dato che il Modello vi fa riferimento, vanno considerati sua parte integrante.

L'Organigramma viene mantenuto sempre aggiornato al fine di assicurare una chiara definizione formale dei compiti assegnati ad ogni unità della struttura della Società.

Opportuna comunicazione dovrà essere inoltrata all'Organismo di Vigilanza (di cui di seguito) per consentire le valutazioni di competenza di quest'ultimo, al fine di stabilire se le variazioni comportino o meno un'incidenza sulla Parte Generale ovvero sulla Parte Speciale del Modello Organizzativo.

Le procedure e istruzioni operative di cui la Società si è dotata mirano a garantire la correttezza e trasparenza della sua attività, da un lato regolando l'agire della stessa, e dall'altro consentendo i controlli, preventivi e successivi, della correttezza delle operazioni effettuate. Ciò in quanto esse favoriscono l'uniformità di comportamento all'interno dell'azienda, nel rispetto delle disposizioni normative che ne regolano l'attività (in relazione a questo aspetto si rinvia al punto successivo, relativo ai Sistemi di Gestione).

Tutti i dipendenti hanno l'obbligo di essere a conoscenza delle norme procedurali interne di specifico interesse della funzione e di rispettarle nell'esercizio dei compiti loro assegnati.

In caso di sostanziale variazione organizzativa, sarà/saranno la/e funzione/i interessata/e ad informare l'Organismo di Vigilanza affinché quest'ultimo possa effettuare le valutazioni di competenza.

Il costante monitoraggio del sistema organizzativo da parte dell'Organismo di Vigilanza consentirà di adattare nel tempo il Modello alle esigenze specifiche, garantendone la dinamicità.

5.2 Il sistema di gestione delle risorse umane

Il personale dipendente è inquadrato a far data dal 01 gennaio 2007 in base al "Regolamento per il personale FORMARE SCARL".

La selezione del personale avviene nel rispetto di una procedura interna. I candidati vengono selezionati in base alla corrispondenza tra le caratteristiche professionali e personali richieste e quelle possedute.

Adeguata attenzione viene rivolta alla formazione del personale, anch'essa gestita secondo una specifica procedura interna.

5.3 Il sistema informativo

Sono in uso nella Società vari applicativi informatici che supportano l'attività dei principali processi interni.

Per garantire la prevenzione dei delitti informatici di cui al D.Lgs. 231/2001, nonché la conformità a quanto previsto dal Regolamento UE 2016/679 e dal D.Lgs. 196/2003, la Società adotta e continuerà ad adottare le seguenti misure:

1. Gestione di accessi, account e profili. Con riferimento alla gestione degli accessi:
   - è prevista la definizione formale, individuale ed univoca, dei requisiti di autenticazione ai sistemi per l'accesso ai dati - i codici identificativi (user-id) per l'accesso alle applicazioni ed alla rete;
   - la corretta gestione delle password è definita da linee guida, comunicate a tutti gli utenti per la selezione e l'utilizzo della parola chiave; (no maiuscole-minuscole e numeri)
   - sono definite apposite regole per la creazione delle password di accesso alla rete, delle applicazioni del patrimonio informativo dell'ente e dei sistemi critici o sensibili (ad esempio: lunghezza minima della password, regole di complessità, scadenza, ecc.);
   - sono individuate modalità specifiche per l'assegnazione dell'accesso remoto ai sistemi, sia da parte dei dipendenti sia da parte di soggetti terzi, quali consulenti, fornitori;
2. Gestione delle reti di telecomunicazione. Con riferimento alla gestione delle reti, sono effettuate verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate.
3. Gestione e sicurezza della documentazione in formato digitale:
   - è regolamentato l'utilizzo della firma digitale nei documenti, disciplinandone responsabilità, livelli autorizzativi, regole di adozione di sistemi di certificazione, eventuale utilizzo ed invio dei documenti, modalità di archiviazione e distruzione degli stessi.
   - vengono effettuate attività di back up dei dati dell'Ente, definendo la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;
   - l'accesso ai documenti informatici già archiviati è consentito solo al personale autorizzato.
4. Nell'espletamento delle proprie attività, tutto il personale dipendente di FORMARE S.r.l., i collaboratori, i consulenti ed eventuali incaricati di FORMARE S.r.l. che hanno accesso alla rete aziendale ed ai Sistemi informativi, sono tenuti ad osservare le seguenti linee guida:
   - non utilizzare i sistemi informatici aziendali per finalità diverse da quelle richieste per l'espletamento della propria attività lavorativa, ove non sia contemplato dalle policy aziendali l'uso promiscuo del bene, o contraria a quanto previsto dal Codice Etico

- evitare l'acquisizione, il possesso e l'utilizzo di software ed hardware, non strettamente necessari per lo svolgimento della propria attività lavorativa, che potrebbero essere adoperati per compromettere la sicurezza dei sistemi informatici;
- evitare l'accesso ad internet e la navigazione per scopi diversi da quelli strettamente necessari allo svolgimento della propria attività lavorativa;
- evitare la diffusione di informazioni relative ai sistemi informatici aziendali;
- non divulgare, fornire o condividere con altri componenti dell'organizzazione o con personale esterno a FORMARE S.r.l. , le proprie credenziali di accesso alla Rete ed ai sistemi aziendali o informazioni in merito alle procedure di controllo utilizzate da FORMARE S.r.l. e dai Fornitori per la rete ed i sistemi aziendali.

5.4 Il sistema dei controlli

5.4.1 Principi, requisiti e livelli di controllo

Con il presente Modello la Società tende a migliorare il proprio sistema di controllo interno, in particolare per le attività a rischio individuate e indicate nella Parte Speciale, Mappa dei Rischi, implementando idonei controlli in grado di riportare i rischi emersi ad un livello di accettabilità. Pertanto, la Società si dota di un sistema in grado di:

- accertare l'adeguatezza dei diversi processi organizzativi interni in termini di efficacia, efficienza ed economicità;
- perseguire l'affidabilità e la correttezza delle scritture contabili e la salvaguardia del patrimonio della Società;
- assicurare la conformità degli adempimenti operativi alle normative interne ed esterne ed alle direttive ed indirizzi interni aventi la finalità di garantire una sana ed efficiente gestione.

Vi possono essere tre livelli di controllo:

- Controlli di primo livello: sono controlli operativi e tecnici quali:
    - controlli informatici, segnalazioni di anomalie ed errori, blocco del flusso procedurale, inseriti all'interno di sistemi procedurali informatizzati che consentono la verifica immediata delle elaborazioni e dei dati da parte di chi ne sta effettuando il trattamento;
    - controlli diretti del responsabile organizzativo, che supervisiona la corretta conduzione delle attività.
- Controlli di secondo livello, effettuati da unità diverse da quelle operative e mirati a verificare la regolarità dell'espletamento delle attività ed il rispetto delle procedure. Possono essere effettuati con sistemi informativi automatizzati e rispondono al principio di separatezza delle funzioni.
- Controlli di terzo livello: sono controlli esterni alla funzione, volti ad individuare le anomalie nei processi e le violazioni delle procedure valutando altresì la complessiva funzionalità del sistema dei controlli interni. Possono essere svolti da soggetti terzi ed indipendenti tra cui l'Organismo di Vigilanza.

A questo sistema di controlli si aggiungono i controlli effettuati da Organismi esterni in modo mirato ed in ambiti specifici. A titolo esemplificativo tali controlli vengono effettuati da ARPA, VVF, Agenzia delle Entrate.

Il sistema di controllo interno si sostanzia quindi in:

- "autocontrollo" o “controlli di primo livello”, eseguito dalle singole funzioni sui propri processi. Tali attività di controllo sono demandate alla responsabilità primaria degli addetti e costituiscono parte integrante di ogni processo organizzativo interno;
- “controllo di compliance”, che comprende i controlli di “secondo” e “terzo” livello, finalizzato a evidenziare e mitigare i rischi di conformità mediante specifiche azioni di monitoraggio.

Il sistema di controllo persegue l’obiettivo di assicurare che siano rispettate le leggi, i regolamenti e le procedure interne, in modo da prevenire la commissione di reati, anche con riferimento alle disposizioni del Decreto. Tale obiettivo viene perseguito mediante:

- la valutazione dell’adeguatezza delle procedure interne a mitigare il “rischio 231”, effettuata in sede di redazione della Mappa dei rischi (di cui alla Parte Speciale del presente Modello);
- un costante monitoraggio, da parte dell’Organismo di Vigilanza, della rispondenza ai principi adottati dalla struttura organizzativa interna, nelle sue procedure e nelle attività poste in essere dalle singole funzioni.

Le componenti del Modello organizzativo devono essere integrate con il sistema di controllo interno, implementato dalla Società, che si basa sui seguenti principi ispiratori:

- chiara assunzione di responsabilità, principio in base al quale qualsiasi attività deve fare riferimento ad una persona o funzione che ne detiene la responsabilità. Tale responsabilità deve corrispondere all’autonomia decisionale ed all’autorità conferita;
- separazione di compiti e/o funzioni, principio per il quale ogni operazione rilevante deve svolgersi attraverso fasi diverse (autorizzazione, esecuzione, contabilizzazione, controllo) affidate a soggetti diversi in potenziale contrapposizione di interessi;
- idonea e formale autorizzazione per complessi omogenei di operazioni rilevanti, ovvero per singole operazioni;
- adeguata registrazione e tracciabilità delle operazioni, principio il cui rispetto consente di individuare le caratteristiche e gli attori dell’operazione nelle varie fasi sopra indicate;
- adeguati procedure interne e flussi di reporting atti a rendicontare le operazioni, in particolare se a rischio;
- adeguati controlli “di secondo livello”, preventivi o consuntivi, sulla correttezza delle attività attraverso verifiche indipendenti sia da parte di soggetti interni all’organizzazione, ma estranei al processo, sia da parte di soggetti esterni (ad esempio OdV).

Il Sistema di prevenzione deve sostanziarsi nell’adeguatezza e nella conoscibilità delle procedure interne affinché il sistema non possa essere aggirato se non intenzionalmente. Conseguentemente nessuno potrà giustificare la propria condotta adducendo l’ignoranza delle direttive ed il reato non potrà essere causato dall’errore umano (per negligenza o imperizia).

Il Sistema di controllo a consuntivo deve essere in grado di rilevare tempestivamente l’insorgere di anomalie attraverso un adeguato monitoraggio dell’attività svolta.

Ciò è in linea con il Decreto, che consente di avvalersi del principio dell’esimente solo in caso di “elusione fraudolenta” per i soggetti apicali; parimenti ed agli stessi fini i controlli interni devono essere implementati in modo tale da garantire in massimo grado l’adempimento degli obblighi di direzione o vigilanza.

5.4.2 Il Controllo sulla gestione economico-finanziaria

Le risorse economico-finanziarie sono gestite nel rispetto delle deleghe e nei tempi programmati: sono altresì previsti controlli periodici infrannuali per evidenziare gli scostamenti dalle previsioni e definire gli eventuali interventi correttivi.
In particolare la Società, in ottemperanza con quanto previsto dall'art. 6, co. 2, lett. c del decreto 231/2001 (obbligo di individuare specifiche modalità di gestione delle risorse finanziarie, idonee ad impedire la commissione di reati), opera in conformità ai seguenti principi:

- separazione e indipendenza delle funzioni aziendali, in raccordo funzionale secondo i criteri di management richiamati nel funzionigramma adottato;
- tutte le operazioni che comportano utilizzazione o impegno di risorse finanziarie devono avere una causale espressa e verificabile ed essere documentate e registrate, con mezzi manuali o informatici, in conformità ai requisiti di correttezza professionale e contabile; il relativo processo decisionale deve essere sempre verificabile e non è consentito in nessun caso che i fondi della Società e la relativa movimentazione possano non essere registrati;
- tutte le operazioni connesse alla gestione finanziaria (incassi e pagamenti) devono essere eseguite mediante l'utilizzo di conti correnti bancari intestati alla Società ed avallati alla firma di un procuratore preventivamente depositata presso l'istituto bancario;
- la gestione di cassa prevede controlli rigorosi dei flussi monetari in entrata, sulla base di riconciliazioni giornaliere tra saldo finale contabile e liquidità presente in cassa;
- giornalmente sono eseguite operazioni di verifica dei saldi e delle operazioni di cassa;
- riguardo ai pagamenti di fatture passive e gli impegni di spesa, sono adottati meccanismi di controllo in base ai quali la fattura viene controllata in tutti i suoi aspetti (corrispondenza, calcoli, fiscalità, ricevimento merce e servizi);
- ogni fattura viene registrata dalla contabilità ed il pagamento non ha luogo senza la preventiva autorizzazione della funzione ordinante.

5.5 Il sistema di controllo della salute e sicurezza dei lavoratori

5.5.1 Principi e requisiti

Preliminarmente si specifica che si è provveduto in via sistematica:

- all'identificazione dei rischi ed alla loro valutazione;
- all'individuazione delle misure di prevenzione e di protezione adeguate rispetto ai rischi riscontrati, affinché questi ultimi siano eliminati ovvero, ove ciò non sia possibile, siano ridotti al minimo – e, quindi, gestiti – in relazione alle conoscenze acquisite in base al progresso tecnico;
- alla limitazione al minimo del numero di lavoratori esposti a rischi;
- alla definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime devono avere priorità sulle seconde;
- al controllo sanitario dei lavoratori in funzione dei rischi specifici;
- alla programmazione della prevenzione, mirando ad un complesso che integri in modo coerente le condizioni tecniche e produttive della società con l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro, nonché alla successiva realizzazione degli interventi programmati;

- alla formazione, all'addestramento, alla comunicazione ed al coinvolgimento adeguati dei destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL;
- alla regolare manutenzione di ambienti, attrezzature, macchine ed automezzi, con particolare riguardo alla manutenzione dei dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Il sistema prevede la puntuale definizione dei compiti, dei doveri e delle responsabilità spettanti a ciascuna categoria di soggetti coinvolti nel settore della SSL, a partire dal Datore di lavoro fino al singolo lavoratore. In questo senso, sono considerati anche i seguenti profili:

- l'assunzione e la qualificazione del personale;
- l'organizzazione del lavoro;
- l'acquisizione dei beni e dei servizi impiegati dalla Società.
- la manutenzione ordinaria e straordinaria delle attrezzature, degli automezzi, dei mezzi di prevenzione e dei dispositivi di protezione collettiva ed individuale;
- l'efficiente gestione delle emergenze;
- le modalità da seguire per affrontare le difformità riscontrate rispetto agli obiettivi fissati ed alle previsioni del sistema di controllo.

Va inoltre rivolta particolare attenzione all'esigenza di predisporre ed implementare, in materia di SSL, un efficace ed efficiente sistema di monitoraggio che, oltre a prevedere la registrazione delle verifiche svolte dalla Società, anche attraverso la redazione di appositi verbali, si sviluppi su un duplice livello, di cui il primo coinvolge tutti i soggetti che operano nell'ambito della struttura organizzativa della Società, ed il secondo è costituito da un controllo esterno affidato all'Organismo di Vigilanza (di cui in seguito).

Per quanto riguarda il controllo di primo livello si rinvia al successivo punto "Monitoraggio", che ne descrive l'attuale articolazione.

Per quanto invece riguarda il secondo livello di monitoraggio, richiamato espressamente dalle Linee Guida di Confindustria, esso deve essere svolto dall'Organismo di Vigilanza, direttamente o tramite soggetti da quest'ultimo delegati.

In ragione della sua idoneità ad assicurare l'obiettività e l'imparzialità dell'operato, nonché l'indipendenza dal settore di lavoro sottoposto a verifica ispettiva, all'Organismo di Vigilanza è assegnato il compito di verificare la funzionalità del complessivo sistema preventivo adottato dalla Società a tutela della salute e della sicurezza dei lavoratori.

Al fine di consentire all'Organismo di Vigilanza di svolgere efficacemente il monitoraggio di secondo livello, è obbligatorio inviare allo stesso copia della reportistica periodica in materia di salute e sicurezza sul lavoro, e segnatamente il verbale della riunione periodica di cui all'art. 35 D.Lgs. n. 81/2008, ove obbligatorio, nonché tutti i dati relativi agli infortuni sul lavoro occorsi nei siti della Società.

I risultati del monitoraggio sono considerati dall'Organismo di Vigilanza ai fini:

- dell'eventuale relazione all'Amministratore Unico per proposte di aggiornamento del Modello, incluso il sistema preventivo adottato dalla Società e le procedure organizzative, in ragione di eventuali inadeguatezze o significative violazioni riscontrate, ovvero di cambiamenti della struttura organizzativa della Società;

- dell'eventuale relazione agli organi/funzioni interne competenti per proposte di irrogazione di sanzioni disciplinari, per l'ipotesi in cui sia riscontrata la tenuta delle condotte indicate nel sistema disciplinare adottato dall'ente ai sensi del Decreto.

Tale complessivo sistema dei controlli applicabili alle attività a rischio, in relazione ai reati in materia di sicurezza e salute nei luoghi di lavoro, è stato definito utilizzando, tra l'altro, le indicazioni contenute nell'art. 30 D.Lgs. n. 81/08.

5.5.2 Organizzazione e ruoli del Servizio Prevenzione e Protezione

Allo stato attuale, il Servizio di Prevenzione e Protezione istituito presso la Società è gestito da personale dipendente, con il supporto di consulenti esterni, ed è così articolato:

- Datore di lavoro (Amministratore Unico);
- Responsabile Servizio Prevenzione e Protezione (RSPP).
- Rappresentante Lavoratori per la Sicurezza (RLS);
- Squadre di "Addetti primo soccorso" ed "Addetti prevenzione incendi";
- Medico competente.

Al fine di prevenire e mitigare i rischi connessi alla sicurezza sul lavoro, la Società impiega criteri prudenziali di qualificazione del personale e principalmente:

- tutti gli impiegati (in funzione dell'attività svolta) sono classificati "video terminalisti", con l'applicazione della conseguente sorveglianza sanitaria e formazione specifica;

5.5.2.1 Nomina del Datore di lavoro

Per quanto attiene al Datore di lavoro, questi coincide, allo stato, con l'Amministratore Unico della Società.

5.5.2.2 Nomina del Responsabile del Servizio Prevenzione e Protezione

Il RSPP è nominato dal Datore di lavoro per l'assolvimento dei seguenti obblighi:

- individuare i Dispositivi di Protezione Individuale da fornire al personale;
- consentire ai lavoratori di verificare, mediante il Rappresentante dei Lavoratori per la Sicurezza, l'applicazione delle misure di sicurezza e protezione della salute;
- consegnare tempestivamente al Rappresentante dei Lavoratori per la Sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'art. 17, lettera a), del D.Lgs. 81/08;
- elaborare il documento di cui all'art. 26, comma 3 e su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia al Rappresentante dei Lavoratori per la Sicurezza;
- consultare il Rappresentante dei Lavoratori per la Sicurezza secondo le disposizioni dell'art. 50 del D.Lgs. 81/08;
- convocare la riunione periodica di cui all'art. 35 del D.Lgs. 81/08, ove prevista;

- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- elaborare le procedure di sicurezza per le varie attività aziendali;
- a proporre i programmi di informazione e formazione dei lavoratori;

Affinché possa concretamente esercitare la delega il RSPP è facoltizzato all'utilizzo diretto ed immediato dei mezzi finanziari idonei. Per eventuali necessità di spesa ingenti dovrà sottoporre un relativo piano di spesa all'Amministratore Unico.

5.5.3 Monitoraggio

Il sistema di monitoraggio attualmente adottato dalla Società coinvolge tutti i soggetti che operano nell'ambito della struttura organizzativa, prevedendo:

- l'auto-controllo da parte dei lavoratori, i quali devono sia utilizzare correttamente le attrezzature di lavoro, i mezzi meccanici, nonché i dispositivi di sicurezza e di protezione messi a loro disposizione, sia segnalare immediatamente le deficienze di tali mezzi e dispositivi nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza;
- il coinvolgimento diretto e costante dei soggetti con specifici compiti in materia di SSL (ad esempio, Datore di lavoro, RSPP), i quali intervengono, tra l'altro, in materia:
    a) di vigilanza e monitoraggio periodici e sistematici sull'osservanza degli obblighi di legge e delle procedure in materia di SSL;
    b) di segnalazione di eventuali deficienze e problematiche;
    c) di individuazione e valutazione dei fattori di rischio nell'ambito dell'organizzazione in cui i lavoratori prestano la propria attività;
    d) di elaborazione delle misure preventive e protettive attuate e richiamate nel Documento di Valutazione dei Rischi, nonché dei sistemi di controllo di tali misure;
    e) di proposizione dei programmi di formazione e addestramento dei lavoratori, nonché di comunicazione e coinvolgimento degli stessi.

Si segnala anche che, in ragione dell'avvenuta adozione, da parte della Società, dei "Sistemi di gestione" integrati (di cui al relativo punto precedente), è previsto l'audit integrato effettuato congiuntamente da un team di dipendenti della Società appositamente formati, col supporto di consulenti esterni.

6 I PROTOCOLLI

6.1 Premessa

I protocolli seguenti esprimono i fondamentali principi di comportamento e/o di controllo, da integrare nel complessivo Sistema di Gestione, per lo svolgimento di specifiche attività a rischio di commissione di reati presupposto. Tali principi costituiscono pertanto altrettanti elementi che devono essere recepiti nelle procedure e nelle attività aziendali.

6.2 Il Protocollo SSL

6.2.1 Attività di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione

Tutti i rischi cui sono esposti i lavoratori, a causa ed in occasione dello svolgimento delle mansioni attribuite, devono essere oggetto di attenta valutazione.

Il Documento di Valutazione dei Rischi (DVR) deve essere predisposto, approvato ed attuato e, necessariamente, deve contenere:

- una relazione sulla valutazione dei rischi per la sicurezza e la salute connessi all'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
- l'indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuale adottati a seguito della valutazione dei rischi;
- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione all'interno della Società che debbono provvedere;
- l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione (RSPP) e del Medico competente che ha partecipato alla valutazione del rischio.
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Il DVR deve altresì rispettare le indicazioni previste da norme specifiche sulla valutazione dei rischi ove concretamente applicabili.

Il Rappresentante dei Lavoratori per la Sicurezza (RLS), ai fini della redazione del DVR, deve essere in ogni caso previamente consultato.

Il DVR deve essere custodito presso l'unità produttiva a cui si riferisce la valutazione dei rischi ed essere aggiornato costantemente in relazione ai mutamenti organizzativi o produttivi rilevanti ai fini della sicurezza e della salute dei lavoratori.

Il DVR è disponibile in azienda e messo a disposizione di chiunque volesse consultarlo. Le misure di prevenzione e protezione adottate devono essere appropriate ed idonee a presidiare i rischi individuati nel DVR.

Le misure di prevenzione e protezione devono essere aggiornate in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza sul lavoro ovvero in relazione al grado di evoluzione della tecnica della prevenzione e della protezione.

Sentito il RSPP, idonei Dispositivi di Protezione Individuale (DPI) devono essere forniti ai lavoratori.

La consegna dei DPI deve essere adeguatamente formalizzata e registrata. I DPI devono essere sottoposti a manutenzione periodica ovvero tempestivamente sostituiti laddove non siano più idonei a garantire adeguata protezione del lavoratore. L'attività di valutazione dei rischi e la predisposizione delle misure di prevenzione e protezione devono essere documentate, tracciate e conservate.

6.2.2 Standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, movimentazioni carichi, etc.

Le specifiche procedure adottate devono essere finalizzate a garantire la sicurezza degli impianti, delle attrezzature e dei luoghi di lavoro; in particolare esistono delle indicazioni, prassi e registrazioni per la gestione dei seguenti processi:

- la manutenzione, la pulitura ed il controllo periodico dei luoghi, degli impianti e delle attrezzature di lavoro;
- le norme generali d'igiene nelle aree di lavoro e nelle aree operative;
- le vie di circolazione e le uscite di emergenza;
- i dispositivi antincendio;
- la fuoruscita di sostanze liquide e gassose;
- le misure di primo soccorso;
- l'utilizzo e la manutenzione dei DPI;
- le modalità di archiviazione e di stoccaggio di prodotti e merci.

La manutenzione e le attività di controllo devono essere documentate e archiviate.

Le procedure finalizzate a garantire la sicurezza dei lavoratori debbono essere adottate con riferimento all'esposizione a specifici rischi tra cui:

- videoterminali;
- agenti fisici;
- agenti chimici;
- agenti biologici;
- agenti cancerogeni;
- movimentazione manuale dei carichi.

Tutta l'attività deve essere documentata e tracciata; i relativi documenti devono essere adeguatamente conservati.

6.2.3 Gestione delle emergenze

I piani di intervento, per far fronte a situazioni di emergenza e di pericolo grave per i lavoratori (es. evacuazione, pronto soccorso, gestione incendi, zone di pericolo, etc.), devono essere individuati. La gestione delle cassette di pronto soccorso o dei kit di primo soccorso, con indicazione dei ruoli e delle funzioni, all'interno dei cantieri, deve essere specificatamente regolamentata.

Il materiale di primo soccorso deve essere costantemente reintegrato in modo tale da garantire in ogni momento la completa ed efficace composizione delle dotazioni. I presidi antincendio devono essere allestiti e devono essere idonei ad evitare l'insorgere di un incendio ed a fronteggiare eventuali situazioni di emergenza, ovvero a limitarne le conseguenze qualora esso si verifichi.

I presidi antincendio devono essere soggetti a controlli periodici e sottoposti ad idonea manutenzione. Il piano di evacuazione deve essere predisposto, attraverso la programmazione degli interventi e l'adozione di provvedimenti/istruzioni, affinché i lavoratori possano, in caso di pericolo grave ed immediato che non può essere evitato, cessare la loro attività ovvero mettersi al sicuro abbandonando, immediatamente, il luogo di lavoro.

Tutta l'attività di gestione delle emergenze (es. prove di evacuazione, controlli sui presidi antincendio, etc.) deve essere documentata, tracciata e conservata.

6.2.4 Sorveglianza sanitaria

Un programma generale di accertamenti periodici per verificare lo stato di salute e l'idoneità dei lavoratori, allo svolgimento della mansione affidata, deve essere elaborato.

Un programma di accertamenti periodici per i lavoratori, esposti a rischi specifici, deve essere elaborato.

Uno specifico canale di informazione, verso i singoli lavoratori finalizzato a comunicare tempestivamente il programma individuale di visite, deve essere istituito.

Adeguate misure, nel caso in cui il lavoratore, tempestivamente avvisato, non si sottoponesse alla visita periodica programmata, devono essere previste.

Laddove, a seguito dell'accertamento sanitario, il lavoratore risultasse inidoneo o parzialmente idoneo a svolgere la mansione affidatagli, è assicurata allo stesso la possibilità di prestare la propria attività lavorativa in termini conformi al proprio stato di salute, qualora fosse possibile nel rispetto da un lato delle esigenze interne e dall'altro della normativa vigente.

Gli incontri periodici con il RSPP devono essere pianificati in base ai bisogni rilevati.

Tutta l'attività relativa alla sorveglianza sanitaria deve essere documentata, tracciata e conservata.

6.2.5 Informazione e formazione dei lavoratori

Specifici corsi di formazione aventi ad oggetto la sicurezza e salute dei lavoratori, devono essere organizzati. I corsi di formazione hanno carattere periodico e sono soggetti ad una programmazione annuale (ivi compresi corsi di formazione per i neoassunti). I corsi di formazione devono avere ad oggetto:

- i rischi specifici cui sono esposti i lavoratori in funzione delle mansioni svolte;
- il corretto utilizzo di macchine, attrezzature e dispositivi di protezione individuale;
- le misure di prevenzione e protezione adottate dall'Ente;
- processi produttivi;
- schemi organizzativi;
- norme interne e procedure operative;

- piani di emergenza.

Un sistema di rilevazione delle presenze idoneo a monitorare che la formazione coinvolga tutti i dipendenti, deve essere elaborato.

Specifiche forme di verifica, finalizzate a verificare il grado di apprendimento dei partecipanti, deve essere somministrato al termine del corso di formazione. Ove la verifica di apprendimento dovesse risultare insufficiente devono essere organizzati corsi di formazione di "recupero".

I lavoratori devono essere informati circa i soggetti responsabili in materia di sicurezza e salute o chiunque altro abbia incarichi specifici al riguardo nonché le modalità di comunicazione con questi ultimi.

Specifici canali di informazione che consentano ai lavoratori, ovvero ai loro rappresentanti, di prospettare eventuali questioni afferenti la sicurezza e salute, devono essere predisposti.

Una opportuna comunicazione deve essere prevista ed altresì rivolta, ai soggetti che occasionalmente accedono presso i luoghi di lavoro ed in particolare al:

- personale esterno (fornitori, committenti, collaboratori esterni);
- pubblico (clienti, visitatori, etc.);
- alle autorità.

Tutta l'attività di formazione ed informazione deve essere documentata, tracciata e conservata.

6.2.6 Attività di vigilanza e controllo

Un piano di verifica annuale, finalizzato a verificare l'adeguatezza dei presidi antinfortunistici, deve essere previsto.

Un piano correttivo qualora, a seguito delle verifiche effettuate, emergessero carenze o, comunque, margini di miglioramento, deve essere definito. Tutte le persone (delegati e preposti) che coordinano l'attività di altri lavoratori devono costantemente verificare:

- la presenza e l'adeguatezza delle misure di prevenzione e protezione;
- il corretto utilizzo dei mezzi di prevenzione e protezione, ove previsti;
- l'adeguatezza nel tempo delle procedure/piani di intervento adottati per la prevenzione infortuni;
- che ai lavoratori siano stati forniti adeguati DPI in relazione alla specifica attività cui sono assegnati;
- che gli stessi utilizzino correttamente i DPI in relazione alla specifica attività cui sono assegnati.

Le segnalazioni fatte dai RLS (Rappresentanti dei Lavoratori per la Sicurezza) devono essere adeguatamente considerate. Qualora, a seguito delle segnalazioni effettuate dai RLS, si ritenessero non necessari interventi correttivi deve essere fornita idonea motivazione a margine della richiesta stessa.

Tutta l'attività di vigilanza e controllo deve essere documentata, tracciata e conservata.

6.2.7 Sistema sanzionatorio

Il non corretto utilizzo dei mezzi di prevenzione e protezione per colpa grave, nonché il mancato utilizzo dei DPI da parte dei lavoratori deve essere specificatamente sanzionato.

Apposite sanzioni per la violazione dei protocolli adottati dalla Società in materia di sicurezza e salute dei lavoratori, devono essere espressamente previste nel sistema sanzionatorio, elaborato a norma del D.Lgs. n. 231/01.

6.3 Il Protocollo per la gestione dei rapporti con la P.A.

Il seguente protocollo è finalizzato a regolamentare la gestione dei rapporti con soggetti pubblici connessi alle seguenti attività:

- adempimenti presso la Pubblica Amministrazione, verifiche ed ispezioni;
- richiesta e gestione di finanziamenti pubblici.

Scopo del presente protocollo è quello di individuare:

- ruoli e responsabilità dei soggetti autorizzati a definire i rapporti con gli Enti Pubblici competenti;
- un sistema di report periodici;
- un sistema di archiviazione della documentazione rilevante, al fine di assicurare la tracciabilità dell'attività svolta.

6.3.1 Adempimenti presso la P.A., verifiche ed ispezioni

Tutti i soggetti che, per ragioni del proprio ufficio, intrattengono rapporti con esponenti o rappresentanti della Pubblica Amministrazione devono gestire tali rapporti personalmente, fornendo le informazioni e i documenti dalla stessa richiesti in sede di verifica o ispezione, ovvero al fine del rilascio di autorizzazioni, licenze o atti amministrativi di altra natura.

Le informazioni o documenti forniti, dovranno essere verificati, ove possibile, dai soggetti designati ovvero, in loro assenza, dai diretti sottoposti precedentemente individuati e, ove possibile, siglati all'atto della consegna.

In assenza del soggetto designato deve essere informato, a cura di colui che per primo intrattiene i rapporti con i soggetti pubblici coinvolti, l'Amministratore Unico che individuerà la persona autorizzata a presenziare all'ispezione/verifica/accertamento. In ogni caso, dell'avvio di una procedura ispettiva deve essere data immediata comunicazione all'Amministratore Unico. Sarà cura di questi valutare l'opportunità di assistere direttamente alla verifica/ispezione.

6.3.2 Richiesta e gestione di finanziamenti pubblici

La richiesta di contributi, finanziamenti, sovvenzioni, ecc. erogati da Enti pubblici ovvero dalla Comunità Europea, impone la predisposizione della documentazione necessaria.

L'istanza di partecipazione deve essere sottoscritta da soggetto munito di poteri di rappresentanza.

I documenti presentati all'Ente pubblico devono essere veritieri.

Le notizie e/o informazioni rilevanti, ai fini della concessione del finanziamento, non possono essere sottaciute.

Il finanziamento pubblico può essere utilizzato unicamente per i fini indicati nel bando.

6.3.3 Modalità di gestione dei flussi informativi

I flussi informativi necessari relativi al presente protocollo sono svolti sulla base dei seguenti principi:

- Tracciabilità. Il soggetto designato alla gestione dei rapporti con la P.A. deve documentare l'attività svolta, mantenendo traccia delle informazioni o dei documenti forniti anche da altre funzioni interne ed indicando i soggetti che hanno eventualmente intrattenuto rapporti con l'ente pubblico coinvolto.
- Verbalizzazione. Il soggetto designato alla gestione dei rapporti, deve predisporre un resoconto relativo all'ispezione/verifica o alla richiesta di erogazione, con allegati gli eventuali verbali redatti dalla P.A. La copia del resoconto deve essere inviato tempestivamente all'Organismo di Vigilanza, nel caso in cui siano emerse criticità.
- Segnalazione criticità. Il soggetto designato deve dare immediata informazione all'Amministratore Unico ed all'Organismo di Vigilanza delle criticità di qualsiasi natura emerse nel corso della gestione delle attività.
- Reportistica. Il soggetto designato, ovvero persona da questi delegata, deve compilare apposito report, relativo alle ispezioni/verifiche/accertamenti/richieste di erogazione, da inviare all'Organismo di Vigilanza nelle periodicità dallo stesso indicate.

  Il flusso informativo ha come scopo quello di permettere all'Organismo di Vigilanza della Società di essere informato su potenziali situazioni a rischio reato e di vigilare sull'applicazione del Modello Organizzativo e del Codice Etico. Tuttavia, laddove nello svolgimento delle attività dovessero emergere criticità di qualsiasi natura, l'Organismo di Vigilanza dovrà essere tempestivamente informato.
- Conservazione della documentazione. Tutta la documentazione relativa alla procedura ispettiva (report, verbale ecc.) o alla richiesta di erogazione deve essere archiviata a cura del soggetto designato e conservata presso la struttura della Società.

6.4 Protocollo per la gestione della contabilità e la formazione del bilancio

Il presente protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di comportamento e di controllo della Società per la gestione della contabilità generale e la predisposizione del bilancio d'esercizio, in conformità con quanto previsto dal D.Lgs. 231/2001.

Quanto definito dal presente protocollo è volto a garantire il rispetto della normativa vigente e dei principi di trasparenza, competenza, correttezza, veridicità, oggettività e tracciabilità nell'esecuzione delle attività inerenti alla gestione della contabilità e della formazione del bilancio.

Il processo di gestione della contabilità e della predisposizione del Bilancio d'esercizio prevede il coinvolgimento secondo le rispettive competenze, di:

- L'Assemblea dei Soci, che provvede all'approvazione del bilancio, approva i criteri di valutazione proposti dall'Amministratore Unico;
- L'Amministratore Unico, che definisce la documentazione necessaria alla determinazione delle componenti valutative, assicura la corretta applicazione dei Principi Contabili applicabili e della normativa di riferimento. In occasione della seduta dell'Assemblea, illustra il Bilancio d'esercizio e lo sottopone all'approvazione dell'Assemblea dei Soci.
- Addetti contabili, che provvedono alla contabilizzazione dei fatti contabili, all'aggiornamento dei registri e dei libri obbligatori di natura contabile ed alla conservazione della documentazione al

fine di garantire la tracciabilità delle operazioni svolte; archiviano, controllano e conservano i registri contabili obbligatori (Libro giornale, Libro inventari, Registri IVA, Registro dei beni ammortizzabili), verificano la correttezza di tutti i movimenti IVA, provvedono alla tenuta del Registro IVA e alla liquidazione periodica della stessa.

La tenuta della contabilità e predisposizione del Bilancio deve articolarsi nelle seguenti attività:

A. tenuta della contabilità generale, la quale ricomprende:
   - gestione e manutenzione del Piano dei Conti;
   - tenuta dei libri contabili obbligatori;
   - registrazione e archiviazione delle fatture passive;
   - emissione e registrazione delle fatture attive;
   - gestione della contabilità generale e altri aspetti contabili (gestione delle operazioni straordinarie sul patrimonio aziendale, gestione della fiscalità, etc.);
B. bilancio d'esercizio, che a sua volta si suddivide in:
   - chiusura del periodo contabile ordinario;
   - raccolta ed elaborazione dei dati contabili di chiusura;
   - valutazione e stima delle poste del bilancio;
   - predisposizione del progetto di bilancio;
   - approvazione del progetto di bilancio annuale.

Le modalità operative per la gestione delle suddette attività, laddove si renderà necessaria, potranno essere disciplinate nell'ambito di ulteriore apposita normativa interna di dettaglio, che dovrà essere sviluppata ed aggiornata a cura dell'ente.

Il sistema di controllo a presidio del processo in oggetto si basa sui seguenti elementi qualificanti a garanzia dell'oggettività e trasparenza delle scelte effettuate:

- Livelli autorizzativi definiti e Separazione delle funzioni;
- Controllo e monitoraggio specifico;
- Tracciabilità delle operazioni e archiviazione.

6.4.1 Livelli autorizzativi definiti e separazione delle funzioni

Il processo di tenuta della contabilità e predisposizione del Bilancio è articolato in varie attività che prevedono l'intervento di soggetti diversi nelle differenti fasi del processo, a garanzia del principio secondo cui nessuno può gestire in autonomia un intero processo, ed in particolare, nel rispetto dei ruoli e responsabilità.

Tutti i soggetti coinvolti nel processo di tenuta della contabilità e della predisposizione del Bilancio di esercizio sono responsabili della completezza ed accuratezza delle informazioni fornite.

Il livello di responsabilità è commisurato ai ruoli e ai compiti effettivamente svolti e presuppongono una chiara formalizzazione dei livelli autorizzativi per la tenuta della contabilità e la predisposizione del Bilancio coerenti con il sistema dei poteri aziendali, tale per cui:

- si prevede la possibilità di effettuare registrazioni contabili limitatamente alle sole risorse dell'Ufficio amministrativo, autorizzate attraverso un sistema di User Id e Password aggiornate periodicamente secondo le vigenti norme sulla sicurezza;
- la gestione del Piano dei conti e i relativi inserimenti/modifiche/eliminazioni di conti contabili è affidata esclusivamente al Amministratore Unico o a personale dell'Ufficio amministrativo previa autorizzazione formale. L'Amministratore Unico autorizza le ulteriori registrazioni da effettuare successivamente alla chiusura della contabilità;
- l'Amministratore Unico, supportato dall'Ufficio amministrativo, redige il Bilancio d'esercizio, da sottoporre a verifica e approvazione dell'Assemblea dei Soci.
- L' Assemblea dei Soci approva il Bilancio d'esercizio nel suo complesso.

6.4.2 Controllo e monitoraggio specifico

Il sistema informativo contabile è dotato dei requisiti necessari ad assicurare il rispetto delle regole di sicurezza, di segregazione delle funzioni e di tracciabilità delle operazioni registrate.

Il sistema informativo utilizzato mantiene traccia dell'operatore che ha effettuato la registrazione contabile.

Nel sistema contabile sono definiti campi obbligatori per le transazioni (data registrazione, data contabile, importo, ecc.) al fine di assicurare che le transazioni incomplete non vengano registrate.

Inoltre, le regole di validazione del sistema contabile non permettono di inserire registrazioni non quadrate.

L'attività di registrazione contabile prevede che ogni operazione sia supportata da adeguata documentazione al fine di rendere dimostrabili i principi di inerenza e competenza ed assicurare che ogni operazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua.

Per quanto concerne la registrazione delle fatture passive, all'arrivo della fattura, i dipendenti dell'ufficio amministrativo effettuano la verifica della corrispondenza con la prestazione/fornitura ricevuta, l'ordine di acquisto e la fattura stessa. In caso di prestazione/materiale non conforme, sentito il referente dell'acquisto per eventuali chiarimenti in merito, richiede al fornitore l'emissione di una nota credito parziale o totale.

6.4.3 Tracciabilità delle operazioni e archiviazione

Tutta la documentazione prodotta a supporto dell'alimentazione della contabilità generale e della predisposizione del Bilancio d'esercizio è archiviata e conservata ai sensi di legge presso l'Ufficio amministrativo.

Gli addetti all'Ufficio amministrativo incaricati all'archiviazione provvedono alla conservazione della documentazione relativa alla tenuta della contabilità al fine di garantire la tracciabilità delle operazioni svolte.

Per quanto attiene alla registrazione delle fatture passive, gli addetti all'Ufficio amministrativo provvedono alla timbratura delle fatture con le seguenti informazioni: numero di protocollo, conto di addebito, conto di accredito, data registrazione.

Gli originali delle fatture sono conservati nell'archivio delle fatture passive.

I registri contabili obbligatori sono conservati presso gli archivi dell'Ufficio amministrativo nei termini previsti dalla legge.

Il Amministratore Unico e i soggetti coinvolti nel processo, ciascuno per la parte di propria competenza, provvedono alla conservazione della documentazione relativa alla chiusura contabile ordinaria al fine di garantire la tracciabilità delle operazioni svolte.

6.4.4 Criteri di comportamento

I soggetti che sono coinvolti nella tenuta della contabilità e predisposizione del Bilancio, sono tenuti ad osservare le previsioni del presente Modello nonché le modalità esposte nel presente protocollo e le disposizioni di legge esistenti in materia.

In particolare, nello svolgimento dei compiti assegnati, gli addetti all'Ufficio amministrativo devono attenersi ai seguenti principi di comportamento:

- assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- garantire un continuo allineamento tra i profili utente assegnati ed il ruolo ricoperto all'interno dell'ente, assicurando il rispetto delle regole di segregazione dei compiti tra il soggetto che ha effettuato l'operazione, chi la registra in contabilità e chi effettua il relativo controllo;
- garantire la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte, archiviando in maniera corretta e dettagliata i documenti di supporto;
- osservare, nello svolgimento delle attività di contabilizzazione dei fatti relativi alla gestione dell'ente, un comportamento corretto, trasparente e collaborativo;
- procedere alla valutazione e registrazione di elementi economico patrimoniali nel rispetto dei criteri di ragionevolezza e prudenza, illustrando con chiarezza, nella relativa documentazione, i criteri che hanno guidato la determinazione del valore del bene;

Nella predisposizione del Bilancio di esercizio i soggetti coinvolti nel processo:

- devono rispettare puntualmente i principi contabili di riferimento;
- nel procedimento di stima devono attenersi al rispetto del principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti, fornendo ogni informazione complementare che sia necessaria a garantire la veridicità del documento;
- predisporre un Bilancio nel rispetto del criterio di completezza sotto il profilo dell'informazione societaria contenenti tutti gli elementi richiesti dalla legge;
- sono tenuti a predisporre la relativa documentazione con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando, e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto d'interesse;
- devono consentire la tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte;
- sono tenuti ad osservare scrupolosamente tutte le norme di legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurano il regolare funzionamento dell'ente e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;

- devono tenere un comportamento corretto, trasparente e collaborativo nei confronti dell'Amministratore Unico, soddisfacendo in modo tempestivo e completo le richieste di documentazione avanzate da quest'ultimo nel corso delle attività di verifica;
- In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:
  - porre in essere attività e/o operazioni volte a creare disponibilità extracontabili, ovvero finalizzate alla creazione di "fondi neri" o di "contabilità parallele", anche se per valori inferiori alle soglie di punibilità di cui agli artt. 2621 e 2622 c.c.;
  - porre in essere azioni finalizzate a fornire informazioni fuorvianti non fornendo una corretta rappresentazione della situazione economica, patrimoniale e finanziaria dell'ente;
  - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta e veritiera della realtà riguardo alla situazione economica, patrimoniale e finanziaria;
  - alterare o distruggere documenti ed informazioni finanziarie e contabili disponibili in rete attraverso accessi non autorizzati o altre azioni idonee allo scopo;
  - omettere di comunicare dati e informazioni imposte dalla legge riguardo alla situazione economica, patrimoniale e finanziaria;
  - ledere l'integrità del patrimonio, in violazione delle disposizioni di legge a tutela dei creditori;
  - occultare documenti ed informazioni;
  - fornire documenti ed informazioni incompleti o fuorvianti;
  - ostacolare in qualsiasi modo lo svolgimento dell'attività di controllo da parte degli organi di controllo in genere;

6.5 I Protocolli generali di prevenzione e sicurezza informatica

6.5.1 Delitti informatici

Trattandosi di reati riferibili generalmente alle modalità con le quali vengono non solo realizzate le attività specifiche dell'azienda ma anche la gestione della medesima, è evidente che il rischio di commissione dell'illecito è astrattamente configurabile in qualunque contesto aziendale. È opportuna pertanto la definizione di standard di comportamento condivisi cui dare ampia diffusione all'interno del contesto aziendale al fine di evitare il rischio della commissione dei suddetti reati.

Per comodità di analisi i delitti informatici possono essere raggruppati nelle seguenti cinque tipologie di reato:

1. Le falsità: documenti informatici (art. 491-bis. c.p.).
2. Delitti contro l'inviolabilità del domicilio: accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.); detenzione o diffusione abusiva di codici di accesso a sistemi informatici a 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.).

3. Delitti contro l'inviolabilità dei segreti: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater); installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies).
4. Delitti contro il patrimonio mediante violenza alle cose o alle persone: danneggiamento di informazioni, dati e programmi informatici (art. 635-bis); danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter); danneggiamento di sistemi informatici o telematici (art. 635-quater); danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies)
5. Delitti contro il patrimonio mediante frode: frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies).

Si tratta dei seguenti reati previsti dal Codice Penale:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici
- Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità
- Falsità ideologica commessa dal privato in atto pubblico
- Falsità in registri e notificazioni
- Falsità in scrittura privata
- Falsità in foglio firmato in bianco. Atto privato
- Falsità in foglio firmato in bianco. Atto pubblico
- Altre falsità in foglio firmato in bianco
- Uso di atto falso
- Soppressione, distruzione e occultamento di atti veri
- Copie autentiche che tengono luogo degli originali mancanti
- Falsità commesse da pubblici impiegati incaricati di un servizio pubblico
- Accesso abusivo ad un sistema informatico o telematico
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche
- Danneggiamento di informazioni, dati e programmi informatici

- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- Danneggiamento dì sistemi informatici o telematici
- Danneggiamento di sistemi informatici o telematici di pubblica utilità
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

6.5.2 Potenziale profilo di rischio rispetto al D. Lgs. 231/2001

I delitti informatici si verificano con comportamenti che realizzano la violazione, il danneggiamento o l'interruzione del sistema informatico interno di FORMARE S.r.l. , di informazioni, dati e programmi informatici di FORMARE S.r.l. e l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni relative al sistema informatico di FORMARE S.r.l..

In questa prospettiva acquistano rilievo tutti i comportamenti che possono compromettere la sicurezza dei sistemi e dei dati informatici e la continuità del servizio informatico nell'ambito di operatività aziendale.

Appare utile ricordare che l'art. 1 della Convenzione sulla criminalità informatica del Consiglio di Europea fatta a Budapest il 23 novembre 2001, ratificata dall'Italia con la legge n. 48 del 18 marzo 2008 definisce "sistema informatico": "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati".

Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di un software che permette il loro funzionamento elaborando delle informazioni (o comandi).

Nel medesimo articolo è contenuta la definizione di "dato informatico" che descrive il concetto derivandolo dall'uso: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informativo di svolgere una funzione".

Come conseguenza della violazione dei sistemi informatici acquistano rilievo le problematiche connesse alla tutela dei dati personali trattenuti dall'azienda. L'analisi dei rischi connessi ai delitti informatici è stata condotta pertanto avendo riguardo ai protocolli specifici di sicurezza dettati dal Regolamento UE 2016/679 in materia di trattamento dei dati personali ed adottati da FORMARE S.r.l. che qui si intendono richiamati.

6.5.3 Principi deontologici e indicazioni comportamentali di riferimento

Nello svolgimento delle attività che comportano accesso al sistema informatico di FORMARE S.r.l. o utilizzo di informazioni e/o dati relativi al sistema informatico di FORMARE S.r.l. si ispira alle disposizioni di legge e ai regolamenti vigenti.

È fatto obbligo ai soggetti coinvolti di non adottare comportamenti a rischio di reato o contrari al Codice di condotta e ai principi di comportamento indicati nel Modello.

In particolare FORMARE S.r.l. si impegna al rispetto dei seguenti principi comportamentali:

- FORMARE S.r.l. , consapevole dei continui cambiamenti tecnologici e dell'elevato impegno operativo, organizzativo e finanziario necessario, si impegna a mantenere un efficace sistema di sicurezza informatica, in particolare attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi, attraverso l'utilizzo di strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attacchi, e (ii) la garanzia della massima continuità del servizio;
- FORMARE S.r.l. e tutti coloro che all'interno o all'esterno di FORMARE S.r.l. sono tenuti a conoscerlo in ragione del loro ufficio (Titolare, Responsabile, Incaricati del trattamento dei dati, oltre a tutti coloro che di fatto trattino dati soggetti alle disposizioni di cui all'art. 34 del D. Lgs. 196/2003) devono uniformare il proprio comportamento alle disposizioni del Regolamento UE 2016/67 in materia di trattamento dei dati personali in FORMARE S.r.l. ;
- l'assegnazione e la gestione delle credenziali di autorizzazione personale (username e password) e delle credenziali di accesso alle diverse sezioni del sistema informatico di FORMARE S.r.l. e i termini di validità delle medesime sono stabilite secondo idonee policy aziendali;
- l'accesso alle diverse sezioni del sistema informatico di FORMARE S.r.l. e a eventuali dati, informazioni, sistemi informatici e telematici cui FORMARE S.r.l. abbia accesso è riconosciuto a dipendenti, collaboratori, consulenti e partner nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico e coerentemente con gli obiettivi aziendali;
- le policy aziendali in materia di accesso al sistema informatico, a eventuali dati, informazioni, sistemi informatici e telematici sono definite dall'Amministratore Unico;
- ogni singolo utente è personalmente responsabile riguardo l'utilizzo del sistema informatico di FORMARE S.r.l. , inclusi eventuali dati, informazioni, sistemi informatici e telematici cui FORMARE S.r.l. abbia accesso, nell'ambito dei presidi posti da FORMARE S.r.l. a tutela della sicurezza, integrità e riservatezza dei dati.

6.5.4 Protocolli di gestione e controllo

Il sistema dei controlli preventivi ai fini dei reati identificati si basa sugli elementi della formalizzata attribuzione di deleghe, della responsabilizzazione dei soggetti delegati, della tracciabilità delle azioni.

In particolare, i protocolli specifici introdotti con riferimento all'attività oggetto di analisi sono di seguito descritti:

- le procedure interne identificano con chiarezza ruoli e competenze delle funzioni incaricate della gestione dei sistemi informatici di FORMARE S.r.l. ;
- il Modello di gestione della privacy (REG UE 679/16) adottato da FORMARE S.r.l. identifica i titolari di permessi di accesso agli archivi cartacei e informatici, distinguendo le misure di sicurezza adottate per i documenti cartacei e per i trattamenti informatici; per questi ultimi sono identificate le procedure adottate per l'autenticazione e l'accesso ai sistemi;

- il Modello di gestione della privacy (REG UE 679/16) adottato da FORMARE S.r.l. prevede un sistema di protezione mediante salvataggio automatico del server della rete aziendale di "backup" su base giornaliera;
- il Modello di gestione della privacy (REG UE 679/16) adottato da FORMARE S.r.l. prevede un sistema di protezione mediante strumenti di "disaster recovery" per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici con frequenza almeno settimanale;
- il sistema informatico è protetto dal rischio di intrusione da parte di virus o di altri software maligni attraverso antivirus con aggiornamento automatico, firewall e proxy;
- è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner che a vario titolo abbiano accesso alla rete aziendale di installare propri software che non rientrino nello scopo per cui il sistema informatico è stato assegnato all'utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale;
- è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner che a vario titolo abbiano accesso alla rete aziendale di installare nella rete propri software che possano impedire o interrompere o danneggiare le comunicazioni informatiche aziendali ovvero l'intero sistema informatico aziendale;
- è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner di operare in maniera illecita su sistemi informativi altrui al fine di sottrarre fraudolentemente dati o informazioni riservate o sensibili;
- i soggetti delegati alla gestione dei sistemi informatici di FORMARE S.r.l. devono annualmente rilasciare all'OdV una dichiarazione attestante la conformità dei comportamenti tenuti con le prescrizioni comportamentali e procedurali indicate nel Modello;
- è fatto obbligo ai soggetti coinvolti di comunicare immediatamente all'OdV l'impossibilità di attuare gli obblighi previsti indicandone la motivazione e ogni anomalia significativa riscontrata nonché ogni evento suscettibile di incidere sull'operatività ed efficacia dell'attività (es. modifiche legislative e regolamenti; mutamenti nell'attività disciplinata, modifica delle struttura e delle funzioni coinvolte, ecc.);
- qualora si verifichino circostanze non regolamentate, che si prestano a dubbie interpretazioni, tali da originare difficoltà nell'operatività dell'attività, è obbligo di tutti i soggetti coinvolti di ricorrere al proprio responsabile che, sentito l'OdV, assume le decisioni del caso.

6.5.5 I reati ex art. 24 bis del D. Lgs. 231/2001 – Protocolli comportamentali

Ai fini dell'attuazione delle regole comportamentali e dei divieti elencati nel punto precedente, i Destinatari della presente, oltre a rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale del presente Modello, devono rispettare i seguenti protocolli comportamentali qui di seguito descritti, posti a presidio dei rischi-reato sopra identificati (art. 24 bis del D. Lgs. 231/2001) e riferibili alle attività sensibili.

I protocolli comportamentali prevedono obblighi (Area del fare) e/o divieti specifici (Area del non fare) che i Destinatari della presente devono rispettare, uniformando la propria condotta ad essi in corrispondenza delle attività sensibili sopra rilevate. Tali principi riprendono, specificandole o, se del caso, integrandole, le norme del Codice Etico e della Parte Generale del Modello. In forza di apposite

pattuizioni contrattuali, i principi in esame si applicano anche ai Soggetti Esterni coinvolti nello svolgimento delle attività sensibili identificate.

Area del Fare

Tutte le attività sensibili devono essere svolte conformandosi alle leggi vigenti, alle norme del Codice Etico, ai principi generali di comportamento del presente Modello, nonché ai protocolli, alle policies e procedure definite e implementate, alle eventuali altre procedure organizzative esistenti poste a presidio dei rischi-reato identificati.

La Società è consapevole del fatto che, per l'attività svolta, la protezione delle infrastrutture IT, dei sistemi informatici/telematici e delle applicazioni, dei dati e delle informazioni ivi contenuti presentano particolare criticità.

In particolare, la Società FORMARE S.r.l. è consapevole che, per il raggiungimento dei propri obiettivi di business e nell'interesse dei suoi stakeholders, è necessario che, mediante un approccio globale, sia garantita la sicurezza delle informazioni, siano attribuite espressamente e formalmente le responsabilità per la sicurezza delle informazioni, venga valutato il livello di sicurezza dei sistemi informatici/telematici con conseguente valutazione e rivalutazione costante del livello di rischio, gestione del rischio medesimo (con l'obiettivo di eliminarlo, mitigarlo o ridurlo comunque al livello ritenuto accettabile) mediante apposite policies, procedure finalizzate alla prevenzione attiva e di rilevamento degli incidenti di sicurezza informatica, nonché adeguata attività di controllo e monitoraggio.

Tale sistema fornisce un modello per la definizione, l'implementazione, il controllo, il monitoraggio e il miglioramento continuo del livello di affidabilità e di funzionamento dei sistemi informatici/telematici aziendali, della protezione delle infrastrutture IT, del patrimonio informativo aziendale e di tutti i dati, ivi comprese le credenziali di accesso, di dipendenti, clienti/utenti e terzi soggetti.

I vantaggi di implementazione di questo sistema di gestione "olistica" della sicurezza informatica/telematica, rappresentati, come detto, da una riduzione dei rischi in termini di probabilità di verificazione e/o di impatto di "incidenti", costituiscono un adeguato presidio anche con riferimento al rischio di commissione dei reati.

Per tale motivo, per il raggiungimento degli obiettivi di prevenzione, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare e attenersi con il massimo rigore a tutte le polizie aziendali e procedure operative.

In particolare:

- la Società definisce, aggiorna, approva formalmente le policies aziendali e le procedure in materia di sicurezza informatica/telematica e ne assicura la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione;
- quanto detto al punto precedente, con particolare riferimento a:
  - piano di business continuity, ivi compreso il disaster recovery;
  - back up (modalità, frequenza, etc.);
  - accesso remoto da parte di terzi soggetti;
  - requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e formalizzazione e tracciatura di tutte autorizzazioni, registrazioni, modifiche e cancellazioni di profili di autenticazione, ivi compresi quelli di clienti/utenti; divieti o limitazioni di accesso a sistemi informatici/telematici, applicazioni o reti;

- generazione, protezione e conservazione dei “log” di sistema, di applicazione e di database;
- concessione di adeguati livelli di privilegio;
- formale assegnazione di particolari livelli di privilegio e formale assunzione della relativa responsabilità;
- controllo e tracciatura di variazioni significative (quantitative e qualitative) di dati e informazioni e altri anomali inserimenti, modificazioni o cancellazioni;
- implementazione, gestione e manutenzione di reti (attribuzione di responsabilità; controlli finalizzati a garantire la protezione e la riservatezza dei dati e delle informazioni ivi contenute, o in transito (vulnerability assessment, penetration test etc.);
- monitoraggio del traffico;
- gestione e manutenzione hardware (ivi compresi inventario e divieti o limitazioni di utilizzo);
- installazione, gestione e manutenzione software e banche dati (ivi compresi inventario, verifica di validità, operatività, scadenza e limiti di licenze e certificazioni di software e banche dati di terzi o loro utilizzo in conformità alle norme sul diritto d’autore e altri diritti
- connessi al suo esercizio; divieti o limitazioni di installazione/utilizzo);
- regolamentazione accesso fisico ai locali in cui risiedono le infrastrutture IT (attribuzione di facoltà di accesso, misure di sicurezza e di vigilanza e assunzione della relativa responsabilità);
- creazione, protezione mediante crittografia (ivi compresa la definizione, distribuzione/segretezza, sostituzione e archiviazione dei relativi algoritmi e chiavi), emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;
- regolamentazione dell’utilizzo della firma digitale con formale attribuzione e formale assunzione della relativa responsabilità.
- Nomina di amministratore/i di sistema e amministratore/i di database con atto formale, definizione di compiti e attribuzioni ed espressa assunzione della relativa responsabilità;
- Per quanto attiene alla sicurezza dei dati personali di tutti i soggetti con i quali intrattiene rapporti a vario titolo, la Società ha adeguato il suo sistema organizzativo ai principi e obblighi di cui alla normativa vigente in materia e, in particolare, del Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), ivi compresa la nomina del Responsabile privacy, e garantisce che il trattamento dei dati medesimi si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
- I sistemi informatici/telematici, i programmi informatici, nonché policies e procedure IT della Società garantiscono che il trattamento dei dati personali avvenga nel rispetto dei principi e norme di cui sopra, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Area del Non Fare

E’ fatto espresso divieto ai Destinatari di porre in essere comportamenti in violazione o comunque non conformi alle policies e procedure definite e implementate dalla Società, nonché comportamenti tali da integrare, anche solo potenzialmente e anche a titolo di concorso o di tentativo, le fattispecie di reato di cui sopra.

In particolare, premesso che:

a) la definizione di "concorso" di persone del reato data dal codice penale ricomprende nel "contributo obiettivamente rilevante" ogni forma di collaborazione, anche "morale", idonea, cioè, determinare o a rafforzare il proposito criminoso di altri soggetti (e.g. istigazione),
b) per documento informatico deve intendersi qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, di natura pubblica o privata, qualora dotato di "efficacia probatoria", cioè con firma elettronica qualificata o emesso nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità,

ai Destinatari è fatto divieto di:

- Formare o concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare documenti informatici falsi o alterare atti veri;
- Contraffare o alterare o concorrere con un p.u. o i.p.s. nel contraffare o alterare certificati o autorizzazioni amministrative contenute in un documento informatico, o a contraffare o alterare le condizioni richieste per la loro validità;
- Concorrere con un p.u. o i.p.s. a formare e rilasciare una copia in forma legale su documento informatico di un atto pubblico o privato inesistente o una copia diversa dall'originale.
- Contraffare o concorrere con un p.u. o i.p.s. nel contraffare un attestato.
- Concorrere con un p.u. o i.p.s. nella falsa attestazione da parte di quest'ultimo in un documento informatico che un fatto è stato da lui compiuto o che è avvenuto in sua presenza, ovvero nell'attestazione da parte dello stesso in un documento informatico di aver ricevuto dichiarazioni non rese o nell'omissione o alterazione di dichiarazioni da lui ricevute;
- Concorrere con un p.u. o i.p.s. nella falsa attestazione, in atti, in certificati o autorizzazioni amministrative sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Concorrere con un esercente una professione sanitaria o forense o altro servizio di pubblica necessità nell'attestare falsamente, in un certificato sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Attestare falsamente, oralmente o per iscritto, ad un p.u. in un atto pubblico, sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Scrivere o lasciare scrivere false indicazioni nelle registrazioni, sotto forma di documento informatico, soggette all'ispezione dell'Autorità di P.S. o nelle notificazioni, sotto forma di documento informatico, alla stessa Autorità, riguardanti operazioni industriali, commerciali o professionali.
- Formare in tutto o in parte scritture private false, sotto forma di documento informatico, o alterazione di scritture private vere, utilizzandole o lasciando che altri le utilizzino.
- Scrivere o far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino.
- Scrivere o far scrivere, ovvero concorrere con un p.u. nello scrivere o nel far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello a cui il p.u. stesso era obbligato o autorizzato.
- Distruggere, sopprimere, occultare in tutto o in parte una scrittura privata o un atto pubblico veri, sotto forma di documento informatico.

- Utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo.

È altresì vietato:

- Introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza.
- Procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo.
- Procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione apparecchiature dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico o le informazioni, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento.
- Intercettare illegittimamente o abusivamente, impedire, interrompere fraudolentemente o illegittimamente comunicazioni informatiche o telematiche.
- Installare illegittimamente o abusivamente apparecchiature atte ad intercettare, impedire, interrompere comunicazioni informatiche o telematiche.
- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui, o utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- Distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero ostacolarne gravemente il funzionamento mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi.

Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o introduzione o trasmissione di dati, informazioni o programmi al fine distruggere, danneggiare, o causare l'inutilizzabilità in tutto o in parte di sistemi informatici o telematici ovvero al fine di ostacolarne gravemente il loro funzionamento.

7 L'ADOZIONE E LA GESTIONE DEL MODELLO

7.1 Adozione e aggiornamento del Modello

L'Amministratore Unico della Società adotta il presente Modello ed informa di tale adozione con specifica comunicazione affissa in bacheca al momento della sua delibera di approvazione.

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a, del Decreto), le successive modifiche ed integrazioni del Modello, effettuate a cura dell'Organismo di Vigilanza (di cui di seguito), sono rimesse alla competenza dell'Amministratore Unico della Società che dovrà procedere alla adozione della versione modificata dello stesso.

Premesso che la modifica del Modello può essere sostanziale o non sostanziale, nei due casi l'approvazione della versione modificata deve avvenire:

- in caso di modifica sostanziale, nel corso della prima riunione utile;
- in caso di modifica non sostanziale, entro sei mesi dall'effettuazione della stessa.

Si considerano modifiche sostanziali del Modello:

- l'introduzione di nuove fattispecie di reato che possono determinare la responsabilità dell'ente ai sensi del Decreto e il conseguente aggiornamento della Parte Generale del Modello e della Mappa dei rischi;
- l'aggiornamento del Sistema di Corporate Governance conseguente a modificazioni adottate della Società;
- l'introduzione di nuovi Sistemi di gestione, oltre a quelli già descritti nel presente Modello;
- la modifica dei protocolli esistenti e l'introduzione di nuovi protocolli;
- la revisione estesa-complessiva della Mappa dei rischi e le relative modifiche alla Parte Generale del Modello.

Tra le modifiche sostanziali, va annoverato inoltre il recepimento delle proposte formulate dall'Organismo di Vigilanza all'Amministratore Unico per gli eventuali aggiornamenti ed adeguamenti del Modello, ritenuti necessari in seguito a violazioni o elusioni delle prescrizioni che mettano in evidenza l'inefficacia del Modello, significative modifiche dell'assetto organizzativo, variazioni normative o orientamenti giurisprudenziali.

Si considerano invece modifiche non sostanziali del Modello tutte quelle non sopra individuate, tra cui principalmente:

- le variazioni al sistema delle deleghe conferite e riportate nel presente Modello, relative sia alla dirigenza sia alla sicurezza;
- le modifiche ai sistemi di gestione già adottati e descritti nel Modello;
- l'aggiornamento/modifica/integrazione della Mappa dei rischi, diversa da quella citata tra le modifiche sostanziali.

7.2 Comunicazione e formazione

7.2.1 Comunicazione

II Modello (Parte Generale e Parte Speciale) è comunicato a ciascuno dei componenti gli Organi sociali, i quali sottoscrivono una dichiarazione di ricevimento, archiviata dall'Organismo di Vigilanza.

Le modalità di diffusione del Modello sono stabilite dall'Organismo di Vigilanza; l'effettiva diffusione è effettuata a cura della Direzione aziendale.

Un estratto della Parte Generale del Modello:

- è affisso nella bacheca aziendale;
- è messo a disposizione di tutti i collaboratori della Società, in forma cartacea presso l'ufficio del Responsabile Risorse Umane;
- è pubblicato sul sito internet della Società.

In generale, sarà cura della Società informare i terzi che interagiscono con l'ente dell'avvenuta adozione del Modello e in sintesi delle parti per essi rilevanti.

Le stesse modalità informative saranno adottate in caso di aggiornamento del Modello, nel momento in cui ne sarà stata data approvazione da parte dell'Amministratore Unico.

7.2.2 Formazione

I principi e i contenuti del Decreto e del Modello sono divulgati mediante corsi di formazione, ai quali tutti i dipendenti ed i collaboratori in generale sono tenuti a partecipare.

La formazione verrà effettuata all'adozione del Modello, a seguito di sue variazioni, nonché ogni qualvolta ciò fosse ritenuto indispensabile dall'Organismo di Vigilanza. La partecipazione ai corsi di formazione è obbligatoria e l'Organismo di Vigilanza vigilerà su tale partecipazione.

La Direzione, di concerto con l'Organismo di Vigilanza, garantirà la necessaria formazione stabilendo:

- il contenuto e la durata dei corsi;
- la loro frequenza;
- i partecipanti e l'obbligo di frequenza;
- le modalità con le quali eseguire i controlli che sia stato realizzato tutto quanto stabilito.

In relazione agli aspetti SSL, la Società attiva – nel rispetto delle previsioni normative – dei piani di formazione differenziati per ruoli e responsabilità, 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; in quest'ottica, particolare rilevanza è riconosciuta alla formazione ed all'addestramento dei soggetti che svolgono compiti in materia di SSL.

L'Organismo di Vigilanza verificherà che la formazione sia tenuta in modo adeguato e che essa sia differenziata nei contenuti, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza dell'ente.

8 L'ORGANISMO DI VIGILANZA E CONTROLLO

8.1 Requisiti e caratteristiche dell'Organismo di Vigilanza

In merito all'organo al quale può essere attribuito il ruolo di vigilanza il Decreto precisa che esso (art. 6, comma 1, lettera b):

- deve essere dotato di autonomi poteri di iniziativa e controllo;
- deve avere compiti di vigilanza sul funzionamento e sull'osservanza del "Modello di organizzazione e gestione";
- deve altresì curarne l'aggiornamento.

Il legislatore non ha tuttavia fornito ulteriori indicazioni circa le caratteristiche specifiche, le responsabilità e la composizione dell'Organismo.

Maggiori indicazioni, sia in merito alla composizione dell'Organismo di Vigilanza (in seguito, anche O.d.V.) che in merito ai requisiti minimi che l'Organismo deve possedere per poter svolgere correttamente i suoi compiti (autonomia e indipendenza, professionalità, e continuità d'azione), sono state fornite dalle linee guida predisposte da alcune associazioni di categoria.

Alla luce delle premesse sopra illustrate, nonché della propria struttura, la Società si dota di un O.d.V., i cui membri sono designati con delibera consiliare e sono rieleggibili. Con la stessa delibera viene fissata la durata della carica (non inferiore a tre anni) ed il compenso.

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e controllo ed ha una posizione indipendente ed autonoma in quanto si relaziona direttamente con l'Amministratore Unico, senza alcun vincolo di subordinazione gerarchica. Per questi motivi, nonché per rispondere al requisito dell'imparzialità, i suoi membri devono essere dotati di onorabilità ed assenza di conflitti d'interesse.

L'indipendenza dei componenti dell'Organismo di Vigilanza viene garantita dal fatto che essi non risultino coniugi, parenti od affini entro il quarto grado degli Amministratori della Società, né legati alla stessa da rapporti di natura patrimoniale.

Il requisito della professionalità dei membri va inteso come capacità specifiche in tema di attività ispettiva e consulenziale, con particolare riferimento alla necessaria competenza legale e di auditing.

I fondamentali requisiti di autonomia, imparzialità, indipendenza, professionalità sono garantiti dal fatto che il solo Amministratore Unico può revocare ciascun membro ovvero l'intero Organismo di Vigilanza, e solo quando si verifichi una giusta causa, e cioè:

- l'interdizione o l'inabilitazione ovvero una grave infermità di uno o più dei componenti che renda l'Organismo di Vigilanza inidoneo a svolgere le proprie funzioni, o un'infermità che, comunque, comporti l'impossibilità a svolgere l'attività per un periodo superiore a sei mesi;
- l'attribuzione ad uno o più dei componenti di funzioni e responsabilità operative incompatibili con i requisiti di autonomia di iniziativa e di controllo, indipendenza e continuità di azione, che sono propri dell'Organismo di Vigilanza;
- un grave inadempimento dei doveri propri dell'Organismo di Vigilanza;
- l'insufficiente vigilanza (qualitativamente o quantitativamente) da parte dell'Organismo (per un periodo superiore ad almeno sei mesi), pur non sussistendo impedimenti di alcun genere allo svolgimento della propria attività;

- una sentenza di condanna della Società ai sensi del Decreto, passata in giudicato, ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art.6, comma 1 lett. d del Decreto;
- l'assoggettamento a misure di prevenzione disposte dall'autorità giudiziaria e secondo la normativa vigente;
- una condanna con sentenza passata in giudicato (salvi gli effetti della riabilitazione):
  - a pena detentiva per uno dei reati previsti in materia bancaria, finanziaria e tributaria,
  - a pena detentiva per uno dei reati previsti nel titolo XI del Libro V del codice civile e nel R.D. n. 267 del 16/03/1942,
  - alla reclusione per un tempo non inferiore a sei mesi per un delitto contro la Pubblica Amministrazione, il patrimonio, l'ordine pubblico e l'economia pubblica,
  - alla reclusione per un tempo non inferiore ad un anno per qualunque delitto non colposo;
- la perdita dei requisiti di indipendenza così come sopra definiti;
- la presenza di un conflitto di interesse permanente.

Tali giuste cause di revoca costituiscono altresì causa di ineleggibilità o di decadenza.

La rinuncia all'incarico, da parte di ciascun membro dell'O.d.V., potrà avvenire in qualsiasi momento con un preavviso di trenta giorni. In tal caso l'Amministratore Unico provvederà in tempo utile alla sua sostituzione.

La decadenza dell'O.d.V. si verifica automaticamente se viene a mancare per dimissioni o altre cause la maggioranza dei componenti.

L'O.d.V. è dotato di autonomo potere di spesa, al fine di potersi avvalere del supporto di professionalità specialistiche esterne nell'esecuzione dei controlli di competenza. A tali fini potrà altresì utilizzare professionalità interne.

L'O.d.V. è comunque obbligato a rendicontare annualmente all'Amministratore Unico l'utilizzo del budget assegnatogli.

Le sopra delineate caratteristiche dell'O.d.V., unitamente alla sua stabilità ed alla possibilità di avvalersi di un suo budget, gli consentono la richiesta continuità d'azione.

Con riferimento all'indipendenza dell'O.d.V., essa è altresì assicurata dall'Amministratore Unico che lo garantisce da rischi di ritorsioni, comportamenti discriminatori o comunque da condotte pregiudizievoli nei suoi confronti per l'attività svolta.

In particolare, qualsiasi atto modificativo o interruttivo nel rapporto con la Società è sottoposto alla preventiva approvazione dell'Amministratore Unico.

8.2 Funzioni, poteri e attività di controllo dell'Organismo di Vigilanza

8.2.1 Funzioni e poteri dell'Organismo di Vigilanza

L'Organismo di Vigilanza è dotato di tutti i poteri necessari per assicurare una puntuale ed efficiente/efficace vigilanza sul funzionamento e sull'osservanza del Modello nonché per l'espletamento dei seguenti compiti:

- verificare il rispetto, l'efficienza, l'efficacia e l'adeguatezza del Modello mediante verifiche periodiche o a sorpresa;
- curare l'aggiornamento della Mappa delle aree interne sensibili nell'ambito delle quali è ipotizzabile la commissione di reati previsti dal Decreto;
- formulare proposte all'Amministratore Unico per gli eventuali aggiornamenti ed adeguamenti del Modello ritenuti necessari in seguito a violazioni o elusioni delle prescrizioni, significative modifiche dell'assetto organizzativo, variazioni normative o orientamenti giurisprudenziali;
- verificare l'attuazione e l'effettiva funzionalità delle modifiche apportate;
- segnalare all'Amministratore Unico le violazioni accertate del Modello che comportino una responsabilità dell'ente e vigilare sulla conseguente applicazione delle sanzioni previste;
- proporre all'organo/funzione competente sia la sanzione sia la sua irrogazione in caso di violazione del Modello;
- raccogliere, elaborare ed archiviare le informazioni rilevanti in ordine al funzionamento ed al rispetto del Modello, nonché la documentazione che compone il Modello medesimo, ivi comprese – inter alia – la Mappa delle aree interne a rischio-reato, i relativi aggiornamenti, le relazioni sull'attività di vigilanza svolta;
- collaborare all'organizzazione di iniziative idonee ad assicurare la massima diffusione e conoscenza delle prescrizioni del Modello, controllando la frequenza ed il contenuto dei necessari programmi di formazione;
- effettuare, direttamente o tramite professionisti, in caso di circostanze particolari (ad esempio, emersione di precedenti violazioni) attività di ricerca e di identificazione di eventuali nuovi rischi.

Coerentemente, all'O.d.V. sono conferiti tutti i poteri necessari per il corretto espletamento dei compiti assegnatigli.

I compiti ed i poteri dell'O.d.V., unitamente alla nomina dei relativi membri, sono oggetto di specifica comunicazione interna.

Per garantire un efficace ed effettivo svolgimento delle proprie funzioni, oltre alle eventuali disposizioni generali dettate dall'Amministratore Unico, tale Organismo ha la facoltà di stabilire apposite regole operative e adottare un proprio regolamento interno al fine di garantire la massima autonomia organizzativa e d'azione del soggetto in questione.

L'attività svolta dall'Organismo di Vigilanza deve essere sempre documentata per iscritto e le sedute verbalizzate e sottoscritte dai suoi componenti.

8.2.2 Attività di controllo dell'Organismo di Vigilanza

L'attività di controllo proprie dell'Organismo di Vigilanza si fondano su:

- verifiche dei principali atti e dei contratti di maggior rilevanza conclusi dalla Società in aree di attività a rischio;
- verifiche delle procedure, al fine di monitorarne l'efficacia e l'effettivo funzionamento in modo da prevenire la commissione dei reati di cui al Decreto;
- verifiche delle segnalazioni ricevute e delle azioni avviate conseguentemente.

8.3 Informativa

8.3.1 Informativa all'Organismo di Vigilanza

L'O.d.V. deve poter disporre di tutte le informazioni necessarie per svolgere efficacemente le proprie funzioni. Ciò comporta che ciascun collaboratore dovrà fornire all'O.d.V. tutte le seguenti informazioni:

- i documenti e le indicazioni relative alle singole attività, ove richiesti;
- le condotte anomale o comunque non in linea con il Modello;
- le notizie relative ad eventuali problematiche nell'effettiva applicazione del Modello nell'ambito delle attività della Società;
- tutte le notizie relative ad apparenti violazioni del Modello:
- eventuali richieste od offerte di denaro, doni (eccedenti il valore modico) o di altre utilità provenienti da, o destinate a, pubblici ufficiali o incaricati di pubblico servizio;
- eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- in base ad un prudente apprezzamento discrezionale della Direzione le notizie relative ai procedimenti disciplinari in corso e alle eventuali sanzioni irrogate ovvero la motivazione della loro archiviazione;
- ogni situazione di pericolo connesso alla salute ed alla sicurezza sul lavoro;
- ogni situazione di pericolo connessa alla preservazione dell'ambiente.

L'informativa di cui sopra dovrà essere completa ed includere la copia della documentazione relativa: la documentazione di supporto, nel caso in cui non sia in possesso dei dipendenti, è ricercata a cura dell'Organismo di Vigilanza in forza dei suoi poteri ispettivi.

La Società garantisce che ciascun collaboratore potrà liberamente contattare l'O.d.V. per segnalare volontariamente le informazioni sopra indicate, con particolare riferimento ad eventuali irregolarità.

Dette informazioni dovranno essere fornite in forma non anonima; qualora invece giungessero in forma anonima, l'O.d.V. ne valuterà la fondatezza.

L'O.d.V. garantisce la necessaria riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge, ed altresì che il segnalante non subisca alcuna forma di ritorsione, discriminazione o penalizzazione. Tuttavia, gli autori di segnalazioni deliberatamente infondate e/o pretestuose potranno essere assoggettati a sanzioni disciplinari.

L'O.d.V. stabilisce inoltre la tempistica con la quale acquisire eventuale documentazione societaria.

Oltre alle segnalazioni sopra descritte, devono essere obbligatoriamente ed immediatamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- 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 previsti dal Decreto o che interessano, anche indirettamente, la Società, i suoi dipendenti o collaboratori e l'Amministratore Unico;
- richieste di assistenza legale inoltrate dai dipendenti o collaboratori e dall'Amministratore Unico in caso di avvio di procedimenti giudiziari per i reati previsti dal Decreto;
- quando reso noto alla Società, l'avvio di procedimenti giudiziari nei confronti dell'Amministratore Unico, di dipendenti, di collaboratori;

- rapporti di controllo dai quali potrebbero emergere fatti, atti, eventi o omissioni con profili di criticità rispetto ai reati previsti dal Decreto.

La Società rende disponibili i necessari canali informativi per consentire la trasmissione di tutte le suddette informazioni all'O.d.V. e li rende noti a tutti i collaboratori con le modalità più opportune.

La violazione degli obblighi di informativa all'Organismo di Vigilanza costituisce violazione del Modello, sanzionabile secondo quanto previsto nell'apposita sezione: "Il Sistema Sanzionatorio".

8.3.2 Le segnalazioni verso l'Organismo di Vigilanza (whistleblowing)

L'Organismo di Vigilanza deve essere informato da parte dei Destinatari su base occasionale, circa ogni altra informazione, di qualsivoglia genere, proveniente anche da terzi ed attinente l'attuazione e la violazione del Modello nelle Aree a rischio di reato nonché il rispetto delle previsioni del Decreto, che possano risultare utili ai fini dell'assolvimento dei compiti dell'Organismo di Vigilanza ("segnalazioni").

In particolare devono essere segnalate le seguenti circostanze:

- condotte illecite, rilevanti ai sensi del Decreto Legislativo 231/01;
- violazioni del Modello, del Codice etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- sospetti di violazioni del Modello, del Codice etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- operazioni societarie o di business per cui si sospetta possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto.

8.3.3 Modalità di trasmissione e valutazione dei flussi informativi e delle segnalazioni

I soggetti segnalanti (lavoratori dipendenti, lavoratori autonomi, Organi statutari, clienti, fornitori), possono accedere all'applicazione informatica dedicata alle segnalazioni attraverso il link "WHISTLEBLOWING" presente sulla home page del portale aziendale www.francialatticini.com oppure accedendo direttamente al seguente indirizzo web: https://formare.whistlelink.com/

Tale piattaforma garantisce, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La gestione esclusiva di questo canale di segnalazione è affidata all'Organismo di Vigilanza (come da specifica procedura). Con riferimento alle modalità di trasmissione delle informazioni/dati/notizie valgono le seguenti prescrizioni.

I Flussi informativi debbono pervenire all'Organismo di Vigilanza ad opera dei responsabili delle diverse funzioni aziendali mediante le modalità definite dall'Organismo medesimo, tra cui la posta elettronica alla casella:

Odvformaresrl@pec.it

oppure indirizzate tramite posta ordinaria a:

Organismo di Vigilanza ex D.Lgs. 231/2001 c/o FORMARE S.r.l.

Via Cornelia, 498 - 00166 Roma (RM)

Le segnalazioni che hanno ad oggetto l'evidenza o il sospetto di violazioni del Modello, del Codice etico o dei Protocolli Preventivi devono pervenire mediante l'apposito sistema di segnalazione predisposto dalla Società.

Le modalità di valutazione e gestione delle segnalazioni è disciplinata da apposita procedura e dal Regolamento di funzionamento dell'Organismo di Vigilanza.

8.3.4 Obblighi e requisiti del sistema di segnalazione (whistleblowing)

Tutti i destinatari (quali a mero titolo di esempio: apicali, sottoposti e terzi che operano nell'interesse o vantaggio della Società), hanno l'obbligo di presentare, a tutela dell'integrità della Società, segnalazioni circostanziate di eventuali condotte illecite, rilevanti ai sensi del D. Lgs. 231/2001, che in buona fede, sulla base della ragionevole convinzione fondata su elementi di fatto, ritengano essersi verificate o di violazioni del Modello di organizzazione e gestione adottato dalla Società, di cui siano venuti a conoscenza in ragione delle funzioni svolte.

Le segnalazioni dovranno essere circostanziate e fondate su elementi di fatto precisi e concordanti.

Il Sistema di segnalazione whistleblowing è organizzato attraverso specifica procedura e un canale alternativo di comunicazione/segnalazione, diverso dal canale inerente i flussi informativi (questi ultimi interni ai sistemi informatici e telematici aziendali), idoneo a garantire, anche con modalità informatiche, la riservatezza dell'identità del segnalante.

In tale ottica, il canale predefinito è una casella di posta elettronica certificata esterna, a cui potranno accedere solamente i componenti dell'Organismo di Vigilanza.

Destinatari apicali hanno il divieto di porre in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

Oltre alle segnalazioni sopra descritte, devono essere obbligatoriamente trasmesse all'OdV, tramite i già citati canali di posta elettronica e di posta ordinaria:

- le informazioni espressamente individuate nella Parte Speciale del presente documento;
- le notizie relative ai procedimenti disciplinari e alle sanzioni erogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

8.3.5 Disciplina del segreto

Nelle ipotesi di segnalazione o denuncia effettuate nelle forme e nei limiti di cui al presente Modello 231 e dettagliati dalla procedura in materia di whistleblowing, il perseguimento dell'interesse all'integrità delle amministrazioni pubbliche e private, nonché alla prevenzione e alla repressione delle malversazioni e degli atti illeciti, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli articoli 326, 622 e 623 del codice penale e all'articolo 2105 del codice civile (come previsto dalla legge vigente).

Quando notizie e documenti che sono comunicati all'organo deputato a riceverli dalla procedura whistleblowing siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce comunque violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

Resta invece fermo l'obbligo di rispettare il segreto professionale e di ufficio per chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con la

Società o gli organi e funzioni preposte alla gestione delle segnalazioni, le quali nel rispetto della vigente procedura whistleblowing (e nell'ambito della propria autonomia e indipendenza) abbiano chiesto pareri specialistici a supporto.

8.3.6 Libri dell'Organismo di Vigilanza

L'OdV stabilisce, tramite il proprio regolamento, le modalità di verbalizzazione delle attività eseguite; tali modalità tengono conto degli obblighi di riservatezza circa i nominativi degli eventuali segnalanti e delle istruttorie di verifica e della facoltà, in capo al Collegio Sindacale (ove nominato) ed al Consiglio di Amministrazione, di consultare i soli verbali delle riunioni e le relazioni periodiche.

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'OdV per un periodo di 10 anni in un'apposita partizione del file server aziendale accessibile dai soli componenti dell'OdV, ovvero in un apposito archivio cartaceo ad accesso selezionato e limitato ai soli stessi componenti dell'OdV.

Le chiavi di accesso all'archivio cartaceo saranno attribuite ai soli componenti dell'OdV, che dovranno restituirle immediatamente al termine del loro incarico per qualsiasi motivo ciò avvenga.

L'accesso ai documenti informatici dell'OdV con poteri di lettura e scrittura dovrà essere consentito esclusivamente ai membri dell'Organismo di Vigilanza stesso.

Interessi dei componenti dell'Organismo di Vigilanza nelle decisioni dell'Organismo stesso

Le modalità di assunzione delle decisioni nel caso in cui uno o più componenti dell'Organismo di Vigilanza siano portatori di un interesse, diretto o indiretto, rispetto ad una decisione da assumere, sono disciplinate all'interno del Regolamento dell'Organismo; per tali casi l'OdV prevede opportuni obblighi di motivazione.

Segnalazioni aventi ad oggetto un componente dell'Organismo di Vigilanza

Le modalità di gestione delle segnalazioni che riguardano uno o più componenti dell'Organismo di Vigilanza sono disciplinate all'interno della procedura whistleblowing.

In tali casi sono previste idonee attività di informazione, verifica ed intervento di altri organi di controllo della Società che assicurano la correttezza dei processi e delle decisioni

8.3.7 Registrazione delle segnalazioni

L'Organismo di Vigilanza stabilisce, tramite il proprio regolamento, le modalità di registrazione delle segnalazioni relative alle violazioni del Modello o di un Protocollo (disciplinate altresì dalla procedura whistleblowing); tali modalità tengono conto degli obblighi di riservatezza circa i nominativi degli eventuali segnalanti e delle istruttorie di verifica, al fine di garantire che tali dati e informazioni non siano consultabili da persone diverse dagli stessi componenti dell'OdV.

8.3.8 Obblighi di informativa da parte dell'Organismo di Vigilanza

Nello svolgimento delle proprie attività, l'Organismo di Vigilanza:

- informa l'Amministratore Unico nel più breve tempo possibile circa le segnalazioni ricevute e le violazioni rilevate in merito a eventi che potrebbero ingenerare responsabilità della Società ai sensi del Decreto;
- presenta all'Amministratore Unico (dopo avere acquisito gli opportuni riscontri dalle strutture interne) una relazione periodica in ordine alle attività di verifica e controllo compiute e dell'esito delle medesime;
- sottopone all'organo dirigente:
  - le carenze organizzative o procedurali rilevate e tali da esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto;
  - la necessità di apportare modifiche e/o aggiornamenti al Modello;
  - le azioni correttive, necessarie o eventuali, da apportare al fine di assicurare l'efficacia e l'effettività del Modello;
  - lo stato di attuazione delle azioni correttive precedentemente deliberate;
- informa, con appropriata tempistica, l'Amministratore Unico, mediante la presentazione di rapporti scritti concernenti aspetti puntuali e specifici della propria attività, ritenuti di particolare rilievo e significato nel contesto dell'attività di prevenzione e controllo;
- riferisce agli organi sopra menzionati specifici fatti od accadimenti, ogni qualvolta lo ritenga opportuno;
- riferisce all'Amministratore Unico circa l'eventuale mancata o carente collaborazione da parte delle funzioni interne nell'espletamento dei propri compiti di verifica e/o d'indagine.

Sono rimesse all'Organismo la calendarizzazione e la regolamentazione della propria attività, ai fini di rispettare i requisiti di continuità d'azione richiesti dalla legge.

Le funzioni interne potranno rapportarsi con l'O.d.V. con la tempistica concordata in funzione delle necessità, per riportare in merito a specifici fatti od accadimenti o per discutere di argomenti ritenuti di particolare rilievo nel contesto della funzione di prevenzione di reati.

Gli incontri dell'Organismo di Vigilanza con l'Amministratore Unico devono essere verbalizzati ed i relativi verbali conservati presso la Società.

9 IL SISTEMA SANZIONATORIO

9.1 Caratteristiche del sistema sanzionatorio

Conformemente alle prescrizioni contenute all'art. 6, punto 2 lett. e) del Decreto ed alle indicazioni di Confindustria, che ha ritenuto nelle proprie Linee Guida l'apparato sanzionatorio quale punto cardine del Modello, è previsto il sistema disciplinare di seguito descritto che prevede apposite sanzioni per la violazione di quanto contenuto nel o richiamato dal Modello, al fine della prevenzione dei reati di cui al Decreto.

Pertanto le norme disciplinari che regolano il rapporto di lavoro a qualsiasi titolo prestato a favore della Società sono integrate da quanto qui previsto.

Ne consegue che saranno considerati come illeciti disciplinari tutte le condotte commissive o omissive, anche colpose, ivi compresa l'omessa informativa all'Organismo di Vigilanza, idonee a ledere l'efficacia del Modello e che a tali condotte saranno applicate le sanzioni di seguito indicate, ferme restando le previsioni di cui alla contrattazione collettiva, ove applicabili.

Il presente sistema sanzionatorio opera nel rispetto delle norme vigenti, incluse quelle previste nella contrattazione collettiva, ove applicabili, ed è aggiuntivo rispetto alle norme di legge o di regolamento vigenti, nonché integrativo delle altre norme di carattere interno, ivi incluse quelle di natura disciplinare.

L'applicazione del sistema è autonoma rispetto allo svolgimento e all'esito del procedimento giudiziario eventualmente avviato presso l'autorità competente.

I soggetti destinatari del presente sistema sanzionatorio potranno esercitare tutti i diritti – ivi inclusi quelli di contestazione o di opposizione avverso il provvedimento disciplinare, ovvero di costituzione di un Collegio Arbitrale – loro riconosciuti da norme di legge o di regolamento, nonché dalla contrattazione, inclusa quella collettiva, e/o dai regolamenti interni.

L'applicazione del sistema sanzionatorio può essere oggetto di richieste di informazioni e di verifiche da parte dell'Organismo di Vigilanza.

Resta inoltre stabilito che il sistema sanzionatorio di seguito riportato è applicabile anche in caso di violazione delle norme in materia di tutela della Salute e della Sicurezza nei luoghi di lavoro; ciò in quanto non siano state previste sanzioni specifiche in caso di violazione delle norme di Prevenzione adottate dalla Società.

Le sanzioni vengono irrogate secondo quanto previsto nel successivo punto, nonché nella contrattazione collettiva, ove applicabile.

9.2 Criteri di graduazione delle sanzioni

L'individuazione del tipo di sanzione e la sua irrogazione avverranno nel rispetto del principio di proporzionalità e di adeguatezza.

Nello stabilire il tipo e l'entità della sanzione verrà tenuto conto:

- dell'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;

- delle altre particolari circostanze che accompagnano la violazione disciplinare, quali modalità della condotta e circostanze nel cui ambito si è sviluppata.

La gravità della condotta sarà valutata, in ordine crescente, a seconda che si tratti di:

- violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve;
- violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave;
- violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato" o "critico", cioè evidenziate in colore giallo o rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave;
- violazione del Modello che integra l'elemento oggettivo e quello soggettivo del dolo, che determina il verificarsi di un reato per il quale il Decreto non prevede la comminabilità di sanzioni interdittive;
- violazione del Modello che integra l'elemento oggettivo e quello soggettivo del dolo, che determina il verificarsi di un reato per il quale il Decreto prevede la comminabilità di sanzioni interdittive (per l'elenco dei reati che prevedono sanzioni interdittive.

Parimenti, relativamente al settore della salute e sicurezza sul lavoro, la gravità della condotta sarà valutata, in ordine crescente, a seconda che si tratti di:

- violazione del Modello che determini una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione;
- violazione del Modello che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- violazione del Modello che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione;
- violazione del Modello che determini una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

Saranno considerate circostanze aggravanti:

- la recidiva;
- il livello di responsabilità assegnato dall'inquadramento contrattuale e organizzativo;
- il concorso di più persone nella commissione della violazione;
- una condotta che dia luogo a più violazioni, la più grave delle quali sarà oggetto dell'aggravamento della sanzione.

9.3 Misure nei confronti dei lavoratori dipendenti

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti sono quelle previste dal sistema disciplinare in vigore, in attuazione di quanto disposto dall'articolo 7 della Legge 20 maggio 1970, n. 300 e con riferimento a quanto previsto in materia disciplinare dal "Regolamento per il personale FORMARE SCARL" del 01 gennaio 2007.

Incorre nel provvedimento del rimprovero, verbale o scritto, il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla Direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello, che comportino la violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve, ovvero che determini una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione.

Incorre nel provvedimento della multa di importo fino ad un massimo di 3 ore di retribuzione, il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla Direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello,

che comportino la violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione.

L'importo delle ritenute per multa sarà introitato dal bilancio dell'Ente e destinato ad attività sociali a favore dei dipendenti.

Incorre nel provvedimento della sospensione dal lavoro e dalla retribuzione per un periodo fino a 5 giorni di effettivo lavoro il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla Direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello

che comportino la violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato" o "critico", cioè evidenziate in colore giallo o rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione.

Incorre nel provvedimento del licenziamento disciplinare senza preavviso il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla Direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello,

che comportino la violazione del Modello realizzata nell'ambito delle aree classificate a rischio "critico", cioè evidenziate in colore rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che

integra l'elemento oggettivo e quello soggettivo del dolo, che determina il verificarsi di un reato per il quale il Decreto prevede la comminabilità di sanzioni interdittive ovvero realizzata in modo da determinare una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

9.4 Misure nei confronti dei componenti l'Organo di Amministrazione e l'Organo di controllo

Qualora sia accertata la commissione di una violazione del presente Modello da parte di uno dei soggetti in discorso, saranno applicate le seguenti sanzioni:

- il richiamo scritto, in caso di violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve, ovvero che determina una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione;
- la diffida al puntuale rispetto del Modello, in caso di violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- la decurtazione degli emolumenti, o del corrispettivo previsto in favore dell'Organo di controllo, fino al 50%, in caso di violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato" o "critico", cioè evidenziate in colore giallo o rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione;
- la revoca dall'incarico, nel caso di condotta in violazione del Modello di gravità tale da far venire meno la fiducia sulla quale è basato il rapporto e da non consentire comunque la prosecuzione, nemmeno provvisoria, del rapporto stesso per comportamenti non conformi alle prescrizioni del presente Modello, che integra l'elemento oggettivo e quello soggettivo del dolo, ovvero realizzata in modo da determinare una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

9.5 Misure nei confronti dei collaboratori esterni

Per collaboratore esterno si intende il personale non dipendente della Società, ma ad esso collegato con rapporto di lavoro parasubordinato.

Le sanzioni previste nei loro confronti sono:

- la diffida al puntuale rispetto del Modello nel caso di violazioni del Modello, ovvero violazioni idonee ad integrare l'elemento oggettivo (fatto) di uno dei reati rilevanti ai sensi del Decreto e l'elemento soggettivo della colpa lieve, ovvero una situazione di concreto pericolo per l'integrità fisica o una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- l'applicazione di una penale in misura pari al 10% del corrispettivo pattuito in favore del collaboratore, nel caso di violazioni idonee ad integrare oltre all'elemento oggettivo (fatto) di uno dei reati rilevanti ai sensi del Decreto anche l'elemento soggettivo della colpa grave, ovvero che

determinino una lesione (v. art. 583, 1° co., Codice Penale), all'integrità fisica di una o più persone, incluso l'autore della violazione;

- la risoluzione del rapporto contrattuale nel caso di violazioni idonee ad integrare oltre all'elemento oggettivo (fatto) di uno dei reati rilevanti ai sensi del Decreto anche l'elemento soggettivo del dolo, ovvero che determinino una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

9.6 Misure nei confronti dei fornitori, partner e consulenti

Ogni violazione delle regole di cui al presente Modello applicabili nei confronti di fornitori, partner e consulenti, ovvero ogni commissione dei reati previsti dal Decreto, è sanzionata secondo quanto indicato nelle specifiche clausole contrattuali da inserirsi nei relativi contratti.

9.7 Rivalsa per risarcimento danni

In ogni caso resta salva l'eventuale richiesta di risarcimento, qualora dai comportamenti sanzionabili derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

9.8 L'irrogazione delle sanzioni

9.8.1 Premessa

Il procedimento di irrogazione delle sanzioni si sviluppa attraverso:

- la fase della contestazione della violazione al soggetto interessato;
- la fase di determinazione e di successiva irrogazione della sanzione.

Si indicano di seguito le procedure di riferimento.

9.8.2 Lavoratori Dipendenti

Fase di contestazione

Il processo sanzionatorio disciplinare ha inizio con la segnalazione effettuata al Responsabile delle Risorse Umane:

- dall'Organismo di Vigilanza; in questo caso nasce da quanto rilevato a seguito di una sua attività ispettiva o similare o da una segnalazione acquisita;
- dal Responsabile di funzione o da qualsiasi altro superiore gerarchico altrimenti denominato ("Responsabile"): in questo caso il Responsabile Risorse Umane provvede ad informare l'Organismo di Vigilanza, il quale potrà effettuare una eventuale, ulteriore attività ispettiva.

Il Responsabile Risorse Umane valuta i fatti con il supporto dell'Organismo di Vigilanza, anche sulla base di eventuali informazioni aggiuntive richieste al Responsabile. A seguito di questa valutazione, qualora non sussistano gli estremi, procederà con l'archiviazione; in caso contrario, passerà alla fase della contestazione scritta della violazione, che verrà approvata dall'Organo di Amministrazione.

La comunicazione dovrà contenere la puntuale indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione nonché l'avviso della facoltà di formulare eventuali deduzioni e/o giustificazioni scritte entro cinque giorni dalla ricezione della comunicazione.

Fase di determinazione ed irrogazione

Valutate le eventuali controdeduzioni (sempre con il supporto dell'Organismo di Vigilanza), l'Organo di Amministrazione passerà se del caso, in base a informazioni del Responsabile Risorse Umane, alla fase della determinazione e applicazione della sanzione.

Il dipendente ha tempo venti giorni dal ricevimento della contestazione per le controdeduzioni; la Società, dal ricevimento delle controdeduzioni, ha tempo venti giorni per irrogare il provvedimento disciplinare.

Il Responsabile Risorse Umane verifica l'applicazione della sanzione nel rispetto delle norme di legge e di regolamento, dei regolamenti interni laddove applicabili, nonché delle previsioni di cui alla contrattazione collettiva.

Il dipendente sanzionato avrà facoltà di adire l'autorità giudiziaria ovvero di promuovere la costituzione di un Collegio di conciliazione ed arbitrato. In tal caso la sanzione disciplinare resta sospesa fino alla pronuncia dell'autorità giudiziaria ovvero del Collegio.

L'Organismo di Vigilanza dovrà essere tenuto informato dall'Organo di Amministrazione dell'irrogazione della sanzione e delle eventuali, successive azioni del dipendente.

9.8.3 Componenti l'Organo di Amministrazione e l'Organo di controllo

Fase della contestazione

Ove un componente l'Organo di Amministrazione non legato alla Società da rapporto di lavoro subordinato violasse il Modello, chiunque rilevasse tale violazione deve darne informativa all'Organismo di Vigilanza.

Questi, effettuati i necessari accertamenti nel tempo più breve, trasmetterà all'Organo di controllo una relazione contenente le seguenti indicazioni:

- identificazione del soggetto responsabile;
- descrizione della condotta con cui sarebbe avvenuta la violazione e delle previsioni del Modello violate;
- documentazione raccolta e altri elementi comprovanti la violazione;
- un'eventuale proposta di sanzione.

L'Organo di controllo deve segnalare all'Assemblea la violazione: entro sette giorni lavorativi dalla ricezione della relazione dell'Organismo di Vigilanza, l'Assemblea deve inviare comunicazione per iscritto, che deve contenere gli estremi della condotta contestata e delle previsioni del Modello che sarebbero state violate, dando facoltà all'interessato di formulare rilievi e/o deduzioni di confutazione.

Ove un componente l'Organo di controllo non legato alla Società da rapporto di lavoro subordinato violasse il Modello, chiunque rilevasse tale violazione deve darne informativa all'Organismo di Vigilanza.

Questi, effettuati i necessari accertamenti nel tempo più breve, trasmetterà all'Organo di amministrazione una relazione contenente le seguenti indicazioni:

- identificazione del soggetto responsabile;

- descrizione della condotta con cui sarebbe avvenuta la violazione e delle previsioni del Modello violate;
- documentazione raccolta e altri elementi comprovanti la violazione;
- un'eventuale proposta di sanzione.

L'Organo di amministrazione deve inviare, entro sette giorni lavorativi dalla ricezione della relazione dell'Organismo di Vigilanza, comunicazione per iscritto, che deve contenere gli estremi della condotta contestata e delle previsioni del Modello che sarebbero state violate, dando facoltà all'interessato di formulare rilievi e/o deduzioni di confutazione.

Fase di determinazione ed irrogazione

L'Organo preposto (Organo di controllo per gli Amministratori, Organo di amministratore per i componenti l'Organo di controllo) deve inoltre convocare rispettivamente l'Assemblea o l'Organo di amministrazione, in tempo utile affinché l'adunanza si tenga entro trenta giorni dalla ricezione della relazione dell'Organismo di Vigilanza. Nel corso di questa adunanza, alla quale dovrà essere invitato a partecipare anche l'Organismo di Vigilanza, dovrà essere disposta l'audizione dell'interessato, che potrà anche presentare le proprie controdeduzioni. Qualora non fossero necessari ulteriori accertamenti, e l'esito comprovasse l'avvenuta violazione, l'Organo preposto determinerà la sanzione da applicarsi e ne fornirà la motivazione; provvederà inoltre a convocare l'Assemblea o l'Organo di amministrazione per le deliberazioni di sua competenza, ove la sanzione consistesse nella decurtazione degli emolumenti o nella revoca dall'incarico.

9.8.4 Collaboratori esterni

Ove un collaboratore esterno violasse il Modello, chiunque rilevasse tale violazione deve darne informativa all'Organismo di Vigilanza.

Questi, effettuati i necessari accertamenti nel tempo più breve, trasmetterà al Responsabile della funzione che gestisce il rapporto contrattuale in questione ed al Responsabile Risorse umane, una relazione contenente le seguenti indicazioni:

- identificazione del soggetto responsabile;
- descrizione della condotta con cui sarebbe avvenuta la violazione e delle previsioni del Modello violate;
- la documentazione raccolta e gli altri elementi comprovanti la violazione;
- un'eventuale proposta di sanzione.

Il Responsabile Risorse umane deve, entro sette giorni lavorativi dalla ricezione della relazione dell'Organismo di Vigilanza, inviare una comunicazione al collaboratore interessato. La comunicazione deve essere effettuata per iscritto e deve contenere gli estremi della condotta contestata e delle previsioni del Modello che sarebbero state violate, dando facoltà all'interessato di formulare rilievi e/o deduzioni di confutazione entro sette giorni dalla ricezione.

Trascorso detto termine, tale funzione, valutate anche le controdeduzioni, comunicherà all'interessato ed all'Organismo di Vigilanza l'esito della procedura e l'eventuale irrogazione della sanzione ritenuta adeguata.

L'Organo di amministrazione provvederà quindi all'effettiva applicazione della sanzione stessa nel rispetto delle norme di legge e di regolamento.

9.8.5 Fornitori, partner e consulenti

La Società applicherà le procedure interne previste in caso di risoluzione contrattuale, ma dell'eventuale irrogazione della sanzione dovranno essere informati, oltre all'Organismo di Vigilanza, anche L'Organo di amministrazione e l'Organo di controllo.

9.9 Conoscibilità

Per garantirne la piena conoscenza da parte di ogni Destinatario, il presente sistema sanzionatorio:

- viene affisso in bacheca ed è tenuto a disposizione presso il Responsabile Risorse umane;
- viene consegnato o inviato per via telematica ai soggetti in posizione apicale ed ai componenti gli Organi societari;
- per quanto di pertinenza, ne viene data appropriata informativa ai collaboratori, consulenti, partner e fornitori.