Modello di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 8 Giugno 2001, N. 231

Parte Generale

Versione n. 02	*Approvata dall'Amministratore Unico con determinazione n. 8 del 4 ottobre 2019*
Versione n. 01	*Approvata dall'Amministratore Unico con determinazione n. 5 del 4 Aprile 2017*

Riferimenti a documenti aziendali:	Piano Triennale di Prevenzione della Corruzione vigente (*sito internet aziendale*)
	Parte Speciale A - Reati nell'ambito dei Rapporti con la Pubblica Amministrazione (*Intranet aziendale*)
	Parte Speciale B - Reati societari (*Intranet aziendale*)
	Parte Speciale C - Reati di lesione colpose gravi o gravissime (Reati in materia di salute e sicurezza sul lavoro) (*Intranet aziendale*)
	Parte Speciale D - Reati informatici e trattamento illecito dei dati (*Intranet aziendale*)
	Parte Speciale E - Reati in violazione di diritto di autore (*Intranet aziendale*)
	Parte Speciale F – Reati ambientali (*Intranet aziendale*)
	Statuto dell'Organismo di Vigilanza (*sito e Intranet aziendale*)
	Tabella reati/illeciti presupposto della responsabilità ex D.lgs. 231/01, con riferimenti legislativi e sanzioni (*Intranet aziendale*)
	Codice Etico (*sito internet aziendale*)
	Organigramma aziendale vigente alla data
Riferimenti esterni:	D.lgs. n. 231/2001 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300" e ss.mm.ii.
	Legge n. 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" e ss.mm.ii.
	D.lgs. n. 231/2007 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e ss.mm.ii.

D.lgs. 33/2013 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" e ss.mm.ii.

D.lgs. 39/2013 “Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190” e ss.mm.ii.

D.lgs. n. 165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche" e ss.mm.ii.

D.lgs. n. 196/2003 “Codice in materia di protezione dei dati personali” e ss.mm.ii.

D.lgs. n. 175/2016 “Testo unico in materia di società a partecipazione pubblica”, come integrato dal D.lgs. n. 100/2017 e ss.mm.ii

Linee Guida di Confindustria per la costruzione dei Modelli di Organizzazione, Gestione e Controllo (approvate 7 marzo 2002 e aggiornate al marzo 2014)

Contratto Collettivo Nazionale dei Lavoratori Metalmeccanici vigente

Legge Regionale n. 42/2006 “Istituzione del Sistema Informativo Regionale Integrato per lo sviluppo della società dell’informazione in Liguria” e ss.mm.ii.

Legge Regionale n. 33/2016 “Disposizioni collegate alla legge di stabilità per l’anno 2017”

Statuto di Liguria Digitale vigente

Patti Parasociali di Liguria Digitale vigenti

Disciplinare Quadro delle attività di Liguria Digitale vigente

Guida pratica per la creazione di un documento Word accessibile" - Redazione a cura dell’Agenzia per l’Italia Digitale (AgID), 18 luglio 2016

Legge n. 179/2017 “Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un

	rapporto di lavoro pubblico o privato" e ss.mm.ii. Regolamento UE n. 2016/679 (GDPR) in materia di privacy e trattamento dei dati personali. D.lgs. n. 101/2018, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679". La legge 9 gennaio 2019, n. 3 "«Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici»"
Moduli utilizzati:	LD17RGE-OdV13-001 "Modello per la segnalazione di condotte illecite"
Revisioni	Il presente documento è stato aggiornato per modifiche all'organizzazione aziendale, del logo aziendale, dei riferimenti normativi e, inoltre, è stato variato il carattere del documento secondo le indicazioni della "Guida pratica per la creazione di un documento Word accessibile", redatta ed emanata dall'Agenzia per l'Italia Digitale (AgID) il 18 luglio 2016 ed inoltre per le nuove disposizioni in materia di Whistleblowing, che non prevedono il completo anonimato ed aggiornamento dei riferimenti normativi.
File	Parte Generale

INDICE

Pag.

1. INTRODUZIONE

1.1. Premessa

La condivisione ed il rispetto dei principi indicati dal D.lgs. 231/01 rappresentano il primo meccanismo preventivo a difesa dell'organizzazione contro qualsiasi tipologia di rischio.

Il Decreto Legislativo n. 231 dell'8 giugno 2001 (indicato di seguito come "Decreto") ha introdotto per la prima volta nell'ordinamento giuridico nazionale la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica.

In base al Decreto, in caso di commissione dei reati ivi specificati, la Società può essere ritenuta direttamente responsabile - unitamente all'autore materiale dell'illecito, che sia un soggetto in posizione apicale dell'Ente o un soggetto posto sotto la direzione o la vigilanza di questi, e che commetta il reato nell'interesse o a vantaggio (esclusivo o concorrente) dell'Ente - qualora non riesca a dimostrare di aver adottato un "Modello di Organizzazione, di Gestione e di Controllo" (di seguito "Modello") tale per cui il soggetto reo, per commettere il reato, abbia dovuto agire eludendo fraudolentemente il modello di organizzazione e di gestione in questione.

Liguria Digitale S.p.A., per assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali nel rapporto con gli Enti Committenti e a tutela delle aspettative dei Soci, ha adottato strumenti organizzativi, di gestione e di controllo, volti a:

- verificare costantemente la conformità delle prassi e delle dinamiche aziendali rispetto alle finalità previste dal Decreto;
- definire e adottare un Modello organizzativo e di controllo coerente alle prescrizioni del D.lgs. 231/01.

Il Modello rappresenta:

- uno strumento di sensibilizzazione per tutti i soggetti che operano per conto della Società, affinché mantengano, nell'espletamento delle proprie attività, comportamenti conformi alle norme esterne e alle regole interne;
- un mezzo di prevenzione contro il rischio di commissione dei reati previsti dal Decreto.

Liguria Digitale, quale Ente di diritto privato in controllo pubblico, è tenuta inoltre ad introdurre e implementare apposite misure organizzative e gestionali ai sensi dalla Legge 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione".

La Società ha quindi predisposto il proprio Piano Triennale di Prevenzione della Corruzione quale documento fondamentale per la definizione della strategia di prevenzione della corruzione e dell'illegalità all'interno della propria organizzazione.

In tal senso, seppur la scelta della Società è stata quella di tenere distinto il Modello 231 dal Piano Triennale di Prevenzione della Corruzione, la coerenza tra i due documenti è garantita sia in termini di finalità, obiettivi, indicatori e risorse associate, sia in termini di modalità e sviluppo dei contenuti.

1.2. Scopo

Il presente documento definisce un complesso organico di principi, regole, disposizioni, schemi organizzativi e connessi compiti e responsabilità, funzionale alla realizzazione ed alla diligente gestione di un sistema di controllo e monitoraggio delle attività sensibili, al fine della prevenzione della commissione, anche tentata, dei reati previsti dal D.lgs. n. 231/2001.

In particolare, il documento si pone l'obiettivo di:

- determinare, in tutti coloro che operano in nome e per conto di Liguria Digitale nelle aree a rischio reato e nelle aree strumentali alla commissione dei reati previsti nel Decreto, la consapevolezza di poter incorrere, in caso di violazione delle norme penali e amministrative ivi indicate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;
- ribadire che tali forme di comportamento illecito sono fortemente condannate da Liguria Digitale S.p.A. in quanto, anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio, sono comunque contrarie alle disposizioni di legge e ai principi di comportamento cui la Società intende attenersi nell'espletamento della propria missione aziendale;
- consentire alla Società, grazie ad una azione di monitoraggio continuo sulle aree a rischio reato e sulle aree strumentali alla commissione dei reati, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

1.3. Area di applicazione

Il Modello si applica a tutti i settori di attività e a tutti i processi aziendali che presentano potenzialmente dei fattori di rischio in relazione alla realizzazione dei reati previsti dal D.lgs. n. 231/01 e pertanto deve essere applicato dai dipendenti di Liguria Digitale S.p.A., dagli Amministratori, dai Collaboratori, ovvero da tutti coloro che abbiano relazioni formali o rapporti contrattuali con la società.

Liguria Digitale S.p.A. non risponde, per espressa previsione legislativa (art. 5, comma 2, Decreto), di azioni compiute dai soggetti soprindicati nell'interesse esclusivo proprio o di terzi.

Il Modello è soggetto a modifiche a seguito di cambiamenti derivanti dall'osservanza delle norme giuridiche in materia e loro integrazioni e variazioni; i principi e le metodologie del presente Modello organizzativo trovano applicazione anche in riferimento a eventuali ulteriori ipotesi di reato successivamente integrate nel Decreto.

1.4. Abbreviazioni

Nel documento vengono utilizzate le seguenti abbreviazioni:

c.c.	Codice Civile
CCNL	Contratto Collettivo Nazionale dei Lavoratori Metalmeccanici
CISO	Chief Information Security Officer
c.p.	Codice Penale
CONSOB	Commissione Nazionale per le Società e la Borsa
D.lgs.	Decreto Legislativo
DPO	Data Protection Officer
Enti Soci	Tutti gli enti che concorrono con Regione Liguria alla partecipazione azionaria dell'azienda
GDPR o RGPD	Regolamento Generale sulla Protezione dei Dati
ICT	Information and Communications Technology
Linee Guida	"Linee guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo - ai sensi del Decreto Legislativo 8 giugno 2001, N. 231" di Confindustria
Liguria Digitale	Liguria Digitale S.p.A.
Modello	Modello di Organizzazione, gestione e controllo ai sensi del D.lgs. 231/01
OdV	Organismo di Vigilanza
PA	Pubblica Amministrazione
PTPC	Piano Triennale di Prevenzione della Corruzione
RPCT	Responsabile della Prevenzione della Corruzione e della Trasparenza

Inoltre, si evidenzia che si intende per:

- **esponenti aziendali**: amministratori, dirigenti e dipendenti Liguria Digitale;
- **soggetti in posizione apicale:** secondo il D.lgs. 231 sono identificati all'art. 5 coloro i quali, indipendentemente dall'attività nominativamente svolta, rivestono di fatto funzioni di rappresentanza, amministrazione o direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché quei soggetti che, anche di fatto, esercitano la gestione e il controllo dell'Ente (organi amministrativi, direttori generali ecc.);
- **sottoposti**: coloro i quali, pur se dotati di autonomia (pertanto passibili di incorrere in illeciti), sono sottoposti alla direzione e alla vigilanza dei soggetti apicali;
- **referenti**: coloro che hanno il compito di trasmettere, tempestivamente o con cadenza relativa al periodo di riferimento, le informazioni rilevanti e i flussi informativi contenuti nelle apposite schede corrispondenti alle attività a rischio di reato processate nel Modello della società.

PARTE GENERALE

2. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 E LA NORMATIVA RILEVANTE

2.1. Il regime di responsabilità amministrativa a carico delle persone giuridiche

Il Decreto Legislativo n. 231 dell'8 giugno 2001, che introduce la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (di seguito il "Decreto"), ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali precedentemente sottoscritte dall'Italia, ed in particolare:

- *la Convenzione di Bruxelles del 26 luglio 1995* sulla tutela degli interessi finanziari della Comunità Europea;
- *la Convenzione di Bruxelles del 26 maggio 1997* sulla lotta alla corruzione di funzionari pubblici sia della Comunità Europea che degli Stati membri;
- *la Convenzione OCSE del 17 dicembre 1997* sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto ha introdotto nell'ordinamento italiano un regime di "responsabilità amministrativa", a carico di società ed associazioni anche prive di personalità giuridica (di seguito denominate "Enti"), per alcuni reati commessi, nell'interesse o a vantaggio degli stessi, da:

- persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi. Si tratta di soggetti che, in considerazione delle funzioni che svolgono, vengono denominati "**apicali**";
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità amministrativa della persona giuridica si aggiunge a quella (penale) della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso (se possibile) del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'Ente permane anche nel caso in cui la persona fisica autrice del reato non sia stata identificata o non risulti punibile.

L'Ente può essere ritenuto responsabile dell'illecito se il reato è stato commesso nel suo **interesse** o a suo **vantaggio**.

Se l'interesse manca del tutto perché il soggetto qualificato ha agito per realizzare un interesse esclusivamente proprio o di terzi, l'impresa non è responsabile. Al contrario, se un interesse dell'Ente - sia pure parziale o marginale - sussisteva, l'illecito dipendente da reato si configura anche se

non si è concretizzato alcun vantaggio per l'impresa, la quale potrà al più beneficiare di una riduzione della sanzione pecuniaria.

Nella decodificazione di tale criterio di imputazione, l'aspetto attualmente più controverso attiene all'interpretazione dei termini "*interesse*" e "*vantaggio*".

Secondo l'impostazione tradizionale, elaborata con riferimento ai delitti dolosi, l'*interesse* ha un'indole soggettiva. Si riferisce alla sfera volitiva della persona fisica che agisce ed è valutabile al momento della condotta: la persona fisica non deve aver agito contro l'impresa. Se ha commesso il reato nel suo interesse personale, affinché l'Ente sia responsabile è necessario che tale interesse sia almeno in parte coincidente con quello dell'impresa.

Per contro, il *vantaggio* si caratterizza come complesso dei benefici - soprattutto di carattere patrimoniale - tratti dal reato, che può valutarsi successivamente (*ex post*) alla commissione di quest'ultimo.

L'argomento è oggetto di un dibattito. Peraltro, la tesi, che tiene distinti interesse e vantaggio anche nei reati colposi pare riflettere più fedelmente il sistema del Decreto 231, che mostra di considerare disgiuntamente i due concetti.

Sul piano soggettivo l'Ente risponde se non ha adottato le misure necessarie ad impedire la commissione di reati del tipo di quello realizzato.

In particolare, se il reato è commesso da soggetti apicali, l'Ente è responsabile se non dimostra che:

- ha adottato ma anche efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione e Gestione idoneo a impedire reati della specie di quello commesso (art. 6, comma 1, lett. a, decreto 231 – vedere anche riferimento puntuale delle caratteristiche del Modello definite al comma 2);
- il compito di vigilare sul funzionamento e l'osservanza del Modello, e di curare il suo aggiornamento, è stato affidato a un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo (OdV che possa fornire evidenza di sufficiente vigilanza);
- il reato è stato commesso per fraudolenta elusione del Modello da parte del soggetto apicale infedele.

Quando il fatto è realizzato da un soggetto sottoposto, la pubblica accusa deve provare che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza da parte degli apicali. Questi obblighi non possono ritenersi violati se prima della commissione del reato l'Ente ha adottato ed efficacemente attuato un modello idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2).

In entrambi i casi (apicale o sottoposto), risultano requisiti essenziali ai fini dell'esimenza le attività di formazione sui protocolli adottati ed il Sistema

Disciplinare collegato ai comportamenti non corretti (art. 6 comma 2 lettera c e art. 7 comma 4 lettera d).

Infine, occorre considerare che la responsabilità dell'Ente può ricorrere anche se il delitto presupposto si configura nella forma del tentativo (art. 26, Decreto 231), vale a dire quando il soggetto agente compie atti idonei in modo non equivoco a commettere il delitto ma l'azione non si compie o l'evento non si verifica (art. 56 c.p.). In tal caso, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà. Inoltre, l'Ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

È importante sottolineare che la responsabilità dell'Ente può sussistere anche laddove il dipendente autore dell'illecito abbia concorso nella sua realizzazione con soggetti estranei all'organizzazione dell'Ente medesimo.

Tale ipotesi è chiaramente rappresentata nel codice penale e, in particolare, negli artt. 110 c.p. e 113 c.p.. Risulta, invece, non altrettanto immediata la sua rilevanza ai fini del Decreto 231.

2.2. Sanzioni

L'accertamento della responsabilità prevista dal Decreto 231 espone l'Ente a diverse tipologie di sanzioni, che, in base al principio di legalità (art. 2 Decreto 231), devono essere individuate dal legislatore.

Sul piano patrimoniale, dall'accertamento dell'illecito dipendente da reato discende sempre l'applicazione di una sanzione pecuniaria e la confisca del prezzo o del "profitto" del reato, anche per equivalente.

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

- sanzioni pecuniarie;
- confisca del prezzo o del profitto del reato;
- sanzioni interdittive;
- pubblicazione della sentenza di condanna.

Le sanzioni pecuniarie

La determinazione delle sanzioni pecuniarie irrogabili ai sensi del Decreto 231 si fonda su un sistema di quote. Per ciascun illecito, infatti, la legge in astratto determina un numero minimo e massimo di quote, sul modello delle cornici edittali che tradizionalmente caratterizzano il sistema sanzionatorio. L'articolo 10 del Decreto 231 si limita a prevedere che il numero di quote non può mai essere inferiore a 100 e superiore a 1000 e che l'importo delle singole quote può oscillare tra un minimo di circa 258 Euro a un massimo di circa 1549 Euro (sanzione minima 25.800 euro, massima 1.549.000 euro)

Sulla base di queste coordinate il giudice, accertata la responsabilità dell'Ente, determina la sanzione pecuniaria applicabile nel caso concreto.

La determinazione del numero di quote da parte del giudice è commisurata alla gravità del fatto, al grado di responsabilità dell'Ente, all'attività eventualmente svolta per riparare le conseguenze dell'illecito commesso e per prevenirne altri. L'importo delle singole quote è invece fissato in base alle condizioni economiche e patrimoniali dell'Ente, al fine di garantire l'effettività della sanzione.

La confisca del prezzo o del profitto del reato

Nei confronti dell'Ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o "*profitto*" del reato, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede.

Quando non è possibile eseguire la confisca sui beni costituenti direttamente prezzo o "*profitto*" del reato, la stessa può avere ad oggetto somme di denaro, beni, o altre utilità di valore equivalente al prezzo o al profitto del reato.

In via cautelare, può essere disposto il sequestro delle cose che, costituendo prezzo o profitto del reato o loro equivalente monetario, sono suscettibili di confisca.

Le sanzioni interdittive

Nei casi previsti dalla legge il giudice penale può applicare le sanzioni interdittive, particolarmente afflittive poiché colpiscono la stessa attività dell'Ente.

A tal fine è necessaria anzitutto l'espressa previsione normativa della possibilità di comminare una sanzione interdittiva a seguito della commissione del reato presupposto in concreto realizzato.

Occorre, poi, che il reato dell'apicale abbia procurato all'Ente un profitto di rilevante entità, che il reato del sottoposto sia stato determinato o agevolato da gravi carenze organizzative oppure che vi sia stata reiterazione degli illeciti.

Le sanzioni interdittive possono consistere:

a) nell'interdizione dall'esercizio dell'attività;

b) nella sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

c) nel divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

d) nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

e) nel divieto di pubblicizzare beni o servizi.

Considerata l'elevata invasività per la vita dell'Ente, le sanzioni interdittive non possono essere applicate dal giudice in maniera generalizzata e indiscriminata.

La pubblicazione della sentenza di condanna

Infine, se applica sanzioni interdittive, il giudice può anche disporre la pubblicazione della sentenza di condanna, misura capace di recare un grave impatto sull'immagine dell'Ente.

La pubblicazione della sentenza di condanna in uno o più giornali, per estratto o per intero, può essere disposta dal Giudice, unitamente all'affissione nel Comune dove l'Ente ha la sede principale, quando è applicata una sanzione interdittiva. La pubblicazione è eseguita a cura della Cancelleria del Giudice competente ed a spese dell'Ente.

2.3. Procedimento di accertamento dell'illecito e sindacato di idoneità del giudice

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale.

Altra regola prevista dal Decreto, ispirata a ragioni di effettività, omogeneità ed economia processuale, è quella dell'obbligatoria riunione dei procedimenti: il processo nei confronti dell'Ente dovrà rimanere riunito, per quanto possibile, al processo penale instaurato nei confronti della persona fisica autrice del reato presupposto della responsabilità dell'Ente.

L'accertamento della responsabilità dell'Ente, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del reato presupposto per la responsabilità della società;
- l'accertamento in ordine alla sussistenza dell'interesse o vantaggio dell'Ente alla commissione del reato da parte del suo dipendente o apicale;
- il sindacato di idoneità sui modelli organizzativi adottati.

Il sindacato del giudice circa l'astratta idoneità del modello organizzativo a prevenire i reati di cui al Decreto è condotto secondo il criterio della c.d. "prognosi postuma". Il giudizio di idoneità è, cioè, formulato secondo un criterio sostanzialmente ex ante, per cui il giudice si colloca, idealmente, nella realtà aziendale nel momento in cui si è verificato l'illecito per saggiare la congruenza del modello adottato.

2.4. Azioni esimenti dalla responsabilità amministrativa

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i reati commessi nell'interesse o a vantaggio dell'Ente sia da soggetti apicali sia da dipendenti.

In particolare, nel caso di reati commessi da soggetti in posizione apicale, l'art. 6 prevede l'esonero qualora l'Ente stesso dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione e di Gestione idoneo a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento è stato affidato ad un Organismo dell'Ente (di seguito "OdV"), dotato di autonomi poteri di iniziativa e controllo;

c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il suddetto Modello;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.

Per quanto concerne i dipendenti, l'art. 7 prevede l'esonero nel caso in cui l'Ente abbia adottato ed efficacemente attuato, prima della commissione del reato, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede, inoltre, che il Modello, debba rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;
- prevedere specifici "Protocolli" (Direttive, Procedure, *Policies*, Linee Guida e in generale il corpo normativo prodotto dalla società,…) 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 di tali reati;
- prevedere obblighi di informazione nei confronti dell'OdV;
- introdurre un "Sistema Disciplinare interno" idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

2.5. I reati-presupposto e le sanzioni previste dal Decreto 231

I reati presupposto e le relative sanzioni previsti dal decreto 231 ed in continuo aggiornamento sono contenuti all'interno del documento "tabella reati/illeciti presupposto della responsabilità ex d.lgs. 231/01, con

riferimenti legislativi e sanzioni", allegata al presente modello, a cui si fa integrale rimando.

3. LINEE GUIDA DI CONFINDUSTRIA[1]

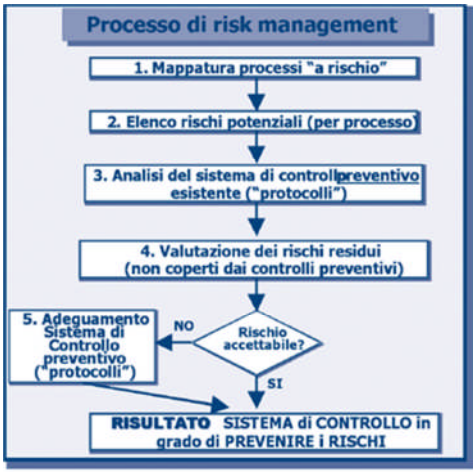
La predisposizione del presente Modello è ispirata alle "Linee guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo - ai sensi del Decreto Legislativo 8 Giugno 2001, N. 231" (di seguito le "Linee Guida") emanate da Confindustria il 7 marzo 2002, integrate in data 3 ottobre 2002 con la "Appendice integrativa in tema di reati societari", successivamente aggiornate in data 31 Marzo 2008 ed infine approvate in data 21 Luglio 2014 dal Ministero della Giustizia.

Il percorso da queste indicato per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

a) **mappatura delle aree a rischio e dei reati rilevanti**: ossia il compimento di una revisione periodica esaustiva della realtà aziendale, con l'obiettivo di individuare le aree che, in ragione della natura e delle caratteristiche delle attività effettivamente svolte, risultano interessate dal potenziale compimento di taluno dei reati contemplati dalla norma

b) **identificazione dei rischi potenziali**: ossia l'analisi del contesto aziendale per individuare in quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente verificare eventi pregiudizievoli per gli obiettivi indicati dal Decreto 231. Per "Rischio" si intende qualsiasi variabile o fattore che nell'ambito dell'azienda, da soli o in correlazione con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi indicati dal Decreto 231 (in particolare all'art. 6, comma 1, lett. a); pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi;

c) **progettazione del sistema di controllo** (cd. "**Protocolli**" per la programmazione della formazione e attuazione delle decisioni dell'Ente), ossia la valutazione del sistema esistente all'interno dell'Ente per la prevenzione dei reati ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi identificati. Sotto il profilo concettuale, ridurre un rischio comporta dover intervenire - congiuntamente o disgiuntamente - su due fattori determinanti: i) la probabilità di accadimento dell'evento e ii) l'impatto dell'evento stesso.



[1] Oltre al codice di comportamento di natura confindustriale non risultano presenti alla data di emissione del presente documento altre guide di riferimento di cui all'art. 6 comma 3 del Decreto.

d) **predisposizione di un sistema di controllo** in grado di ridurre i rischi attraverso l'adozione di appositi protocolli. A supporto di ciò soccorre l'insieme coordinato di strutture organizzative, attività e regole operative applicate – su indicazione del vertice apicale – dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno.

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

- Codice Etico;
- sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro;
- procedure manuali ed informatiche (sistemi informativi);
- poteri autorizzativi e di firma;
- comunicazioni al personale e sua formazione.

Il sistema di controllo inoltre deve essere uniformato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal Modello;
- individuazione dell'OdV i cui principali requisiti siano:
  - autonomia ed indipendenza;
  - professionalità;
  - continuità di azione;
- obbligo da parte delle funzioni aziendali, e soprattutto di quelle individuate come maggiormente "a rischio", di fornire informazioni all'OdV, anche su base strutturata, e di segnalare anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (in quest'ultimo caso l'obbligo è esteso a tutti i dipendenti senza seguire linee gerarchiche).

4. DESCRIZIONE DELL'AZIENDA – ELEMENTI DEL MODELLO DI GOVERNANCE

4.1. Storia e Attività di Liguria Digitale

Liguria Digitale, già Datasiel S.p.a. costituita ai sensi della L.R. 9 aprile 1985, n. 17, divenuta dal 1 gennaio 2015 Società Consortile per Azioni a seguito di trasformazione in conformità con l'art. 12 della L.R. 5 Agosto 2014 n. 20, è oggi una Società per Azioni.
In data 14 Marzo 2017, infatti, ai sensi dell'art. 3 della L.R. del 27 dicembre 2016 n. 33, l'assemblea straordinaria dei Soci ha deliberato la trasformazione della Società Consortile per Azioni Liguria Digitale in Società per Azioni. Detta trasformazione, ai sensi e per gli effetti dell'art. 2500 *novies* del c.c., è efficace dal 1 giugno 2017.

La Società è strutturata al servizio della Regione Liguria e degli Enti Soci che esercitano sulla stessa, secondo il modello dell'"*in house providing*" stabilito dall'ordinamento interno e dall'Unione Europea, il controllo analogo a quello esercitato sulle proprie strutture organizzative.

Liguria Digitale svolge per i Soci le attività previste dalla legge (attività di sviluppo, conduzione e gestione del SIIR, costituenti servizi di interesse generale, art. 10, comma 3, L.R. 42/2006) e dallo Statuto, secondo le modalità stabilite dal Disciplinare Quadro e dai Patti Parasociali.

La Società è quindi vincolata a realizzare oltre l'80% del proprio fatturato nei confronti e nell'interesse della Regione Liguria, degli Enti Soci e dei loro organismi ausiliari, per i quali opera "al costo". Può inoltre svolgere attività per Enti terzi, pubblici o privati, non soci, nel limite di una percentuale di fatturato inferiore al 20%, come espressamente previsto dall'art. 16 del D.lgs. n. 175/16 ("Testo unico in materia di società a partecipazione pubblica" e ss.mm.ii.), solo a condizione che la stessa permetta di conseguire economie di scala o altri recuperi di efficienza sul complesso dell'attività principale della società.

Quale organismo partecipato dalla Regione Liguria e dagli Enti pubblici Soci, ha lo scopo di perseguire il miglioramento qualitativo nella gestione pubblica mediante la realizzazione e la messa a disposizione degli operatori pubblici di un sistema integrato di servizi informativi ed informatici e la diffusione di una cultura dell'informazione quale fonte di sviluppo sociale e tecnologico.

La Società svolge inoltre compiti di supporto alla programmazione, assistenza tecnica e consulenza per lo sviluppo della società dell'informazione in Liguria e sulle soluzioni ICT per il sistema pubblico ligure, nonché di promozione dell'innovazione ICT sul territorio anche attraverso iniziative interregionali, nazionali ed europee attuate dalla Regione Liguria e dagli Enti Soci.

A tal fine le attività della Società hanno in particolare ad oggetto:

- il supporto alla programmazione, assistenza tecnica e consulenza per lo sviluppo della società dell'informazione in Liguria anche nell'ambito di iniziative interregionali, nazionali ed europee;
- la progettazione, la messa in opera e la gestione operativa di progetti di innovazione basati anche su sistemi informativi, la razionalizzazione di sistemi già in esercizio;
- la produzione di sistemi operativi, procedure e programmi elettronici sia di base che applicativi:
- l'organizzazione, la realizzazione, la messa in opera e la gestione operativa di strutture logistiche attrezzate, impianti speciali, apparecchiature elettroniche e quanto altro necessario per la realizzazione e il funzionamento di impianti informatici;
- la manutenzione di sistemi informativi ivi inclusa l'effettuazione di controllo e diagnostiche di efficienza
- la messa in servizio dei sistemi sia per quanto attiene le procedure che le apparecchiature, la realizzazione e la diffusione di prodotti e servizi informatici;
- il dispiegamento di infrastrutture tecnologiche abilitanti la connettività, l'interoperabilità e la cooperazione applicativa;
- ogni attività inerente all'innovazione tecnologica e funzionale degli Enti Soci in esse incluse le attività formative e la ricerca di base e applicata connesse alle attività di cui sopra.

La Società per gli Enti Soci:

- svolge attività di comunicazione, multimediali e di produzione di contenuti editoriali e opera in raccordo con il sistema di istruzione e formazione, per la promozione dell'innovazione ICT sul tenitorio ligure attraverso l'animazione di community, la creazione di competenze, lo sviluppo di start-up;
- eroga in outsourcing servizi al cittadino e servizi amministrativi basati sull'utilizzo di sistemi ICT;
- provvede, quale amministrazione aggiudicatrice e centrale di committenza a tutti gli appalti comunque connessi allo svolgimento delle sue attività, sia per ottimizzazioni interne sia per Regione Liguria e gli Enti Soci, secondo le norme ed i principi specificamente applicabili alle società cosiddette "*in house providing*".

Per il raggiungimento dello scopo sociale, nei limiti consentiti dal modello "*in house providing*" la Società può compiere tutte le operazioni, industriali, commerciali, finanziarie, mobiliari ed immobiliari, nonché le attività direttamente o indirettamente connesse all'oggetto sociale, compreso il

rilascio di fidejussioni, l'acquisizione, cessione e sfruttamento di privative industriali, brevetti, invenzioni in base alle linee di indirizzo stabilite nella programmazione regionale.

La Società per Enti terzi, pubblici o privati, non soci e nei limiti indicati dalla legge (D.lgs. n. 175/16) può:

- svolgere attività di sviluppo del Portafoglio Clienti con riferimento all'intera gamma di prodotti, servizi e soluzioni aziendali. Obiettivo di tali attività è espandere la quota di business della Società nel mercato curando i rapporti e le relazioni di business verso clienti, fornitori, partner, enti ed istituzioni in ambito locale, nazionale e internazionale e coordinando la promozione e l'aggiornamento del Catalogo Prodotti & Servizi, anche nell'ottica della massima valorizzazione dell'expertise aziendale.
- erogare in outsourcing varie tipologie di servizi alle imprese basati sull'utilizzo di sistemi e infrastrutture ICT (servizi Data Center di Outsourcing, Housing, Hosting, Cloud Computing e Consulenza);
- procedere alla gestione degli acquisti di beni e servizi sul mercato utili alla predisposizione di preventivi e offerte finalizzate al conseguimento di economie di scala o altri recuperi di efficienza sul complesso dell'attività principale della Società (secondo le norme ed i principi specificamente applicabili alle società "a controllo pubblico" che svolgano attività "in regime di economia di mercato").

Nel settembre 2019 la Società, dopo avere adottato specifiche Politiche e Procedure, ha ottenuto le certificazioni di conformità alla norma ISO 14001:2015 (Sistema di Gestione Ambientale) ed ISO 45001:2018 (Sistema per la Salute e Sicurezza del lavoratori) con l'ente di certificazione URS Italia per la sede del Data Center, sito in Via Scarsellini 40, Genova.

Nota: la società non ha partecipazioni o forme di controllo/direzione così come definite dal Codice Civile su altre società, soggetti giuridici o Enti.

4.2. Modello di Governance

La *Governance* di Liguria Digitale si impernia sul fatto che attualmente l'azionariato è interamente composto da Regione Liguria e dagli Enti Soci i quali esercitano sulla Società il controllo analogo a quello esercitato sulle proprie strutture organizzative e in relazione ai servizi dalla stessa prestati nei loro confronti. Le modalità di esercizio del controllo analogo ed il modello di *Governance* ad esso correlato sono stabilite dallo Statuto sociale.

La Società è oggi a totale capitale pubblico e la maggioranza assoluta del capitale sociale è detenuta da Regione Liguria.

Gli organi societari sono nominati dalla Regione e dagli Enti Soci, sulla base delle modalità indicate dallo Statuto sociale ed in conformità con la normativa vigente.

Gli organi della Società sono:

- **Amministratore Unico**. La Società è amministrata da un Amministratore Unico nominato ai sensi dell'art. 2449 c.c. dalla Regione Liguria. L'Amministratore Unico dura in carica per il periodo stabilito dall'Assemblea dei Soci e comunque non superiore a tre esercizi. Scade ai sensi dell'art. 2383 secondo comma c.c. ed è rieleggibile. L'Amministratore unico è investito dei poteri per l'amministrazione della Società e, più segnatamente, ha facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione ed il raggiungimento degli scopi sociali, esclusi soltanto gli atti che la legge e lo statuto riservano all'Assemblea e fermo restando l'esercizio del controllo analogo congiunto da parte di tutti i Soci. L'Amministratore Unico ha la rappresentanza legale della Società, nonché la firma sociale. Il potere di rappresentanza e di firma può anche essere conferito, nelle forme di legge, a procuratori speciali per il compimento di specifici atti e di categorie di atti;
- **Collegio Sindacale**. Il Collegio dei Sindaci si compone di tre membri effettivi e di due supplenti, rieleggibili, nominati nel rispetto delle norme a tutela della rappresentanza di genere. La Regione Liguria, ai sensi e per gli effetti dell'articolo 2449 c.c., nomina almeno due membri effettivi ed almeno un membro supplente. Ai soci di minoranza spetta in ogni caso la nomina di un membro effettivo e di un membro supplente da scegliersi nelle modalità previste in apposito regolamento assembleare. Il Presidente del Collegio Sindacale deve essere scelto tra i sindaci nominati dalla Regione Liguria. Al Collegio Sindacale spetta il compito di vigilare sull'osservanza della legge e dello statuto, sul rispetto dei princìpi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento (art. 2403 c.c.);
- **Direttore Generale**. Può essere nominato dall'Amministratore Unico un Direttore Generale a tempo determinato. Tale incarico cessa con la scadenza dell'Amministratore Unico che ha proceduto alla nomina. L'Amministratore Unico, all'atto della nomina del Direttore Generale, ne stabilisce i poteri. Il Direttore Generale è preposto all'esecuzione delle disposizioni generali impartite dall'Amministratore Unico ed è responsabile della gestione operativa della Società e dell'organizzazione aziendale. Il Direttore Generale ha la rappresentanza della Società con riferimento ai propri poteri;
- **Assemblea dei Soci**. L'Assemblea dei Soci rappresenta la universalità dei Soci e delibera in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla Legge o dallo Statuto.

La revisione legale dei conti è esercitata da un revisore contabile o da una **Società di Revisione** iscritti nel registro di legge. L'incarico della revisione

legale dei conti è conferito, sentito il Collegio Sindacale, dall'Assemblea, la quale determina il relativo corrispettivo per tutta la durata dell'incarico.

Inoltre sono costituiti:

- uno "Steering Commitee" con compiti decisionali di tipo strategico. I componenti di diritto dello Steering Commitee sono l'Amministratore Unico, il Direttore Generale, i Direttori delle Direzioni di Business e il Direttore della struttura "Administration, Finance & Control". L'invito a presenziare potrà essere esteso anche ad altri soggetti, sulla base degli argomenti affrontati dal Comitato;
- un Internal Audit che, in ottemperanza all'art. 6, comma 3 lettera b, del Decreto Legislativo n. 175/2016 «Testo unico in materia di società a partecipazione pubblica», opera quale strumento dell'organo amministrativo per prestare attività di verifica dell'operatività e dell'idoneità del sistema di controllo interno e di gestione dei rischi, attraverso un piano di audit basato su un processo strutturato di analisi e prioritizzazione dei principali rischi;
- un "presidio del Risk Management creditizio e finanziario" che opera a diretto riporto del Direttore Generale, con il compito di predisporre specifici programmi di valutazione del rischio aziendale ai fini dell'individuazione di situazioni che qualifichino una "soglia di allarme". Tali programmi devono essere comunicati all'Assemblea dei Soci nell'ambito della relazione di accompagnamento al Bilancio di esercizio di Liguria Digitale;
- un DPO (Data Protection Officer) che, in attuazione a quanto prescritto dagli articoli 38 e seguenti del Regolamento Europeo 2016/679 in materia di protezione dei dati personali, è deputato a informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento stesso, predisponendo le necessarie iniziative formative, le attribuzioni di responsabilità, la valutazione d'impatto sulla protezione dei dati, nonché cooperando con l'autorità di controllo anche fungendo da punto di contatto;
- un Chief Information Security Officer (CISO) deputato, con una visione sistemica, al contrasto delle minacce informatiche e al governo dei rischi ad esse correlati
- un Gestore delle segnalazioni Antiriciclaggio, in applicazione del D. Lgs. 231/2007 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione", come modificato dal D.lgs. n. 90/2017.

4.3. Assetto organizzativo

La struttura organizzativa della Società è ispirata al principio della separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo.

La struttura organizzativa aziendale è definita sulla base di Ordini di Servizio emessi dal vertice aziendale; l'Organigramma di sintesi, consultabile sulla Intranet aziendale, è riportato nell'Allegato 1 del Modello.

5. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ADOTTATO DA LIGURIA DIGITALE

Liguria Digitale, al fine di assicurare che il comportamento di tutti coloro che operano per conto o nell'interesse della Società sia sempre conforme ai principi di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha adottato un Modello di Organizzazione, Gestione e Controllo in linea con le prescrizioni del Decreto, nonché sulla base delle Linee Guida emanate da Confindustria.

Tale iniziativa, unitamente all'adozione del Codice Etico, è stata assunta nella ferma convinzione che l'adozione del Modello di Organizzazione, Gestione e Controllo costituisca un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano nell'interesse o a vantaggio di Liguria Digitale.

In particolare, si considerano Destinatari del presente Modello e, come tali e nell'ambito delle specifiche competenze, tenuti alla sua conoscenza ed osservanza:

- l'Amministratore Unico, nel fissare gli obiettivi, decidere le attività, realizzare i progetti, proporre gli investimenti e in ogni decisione strategica relativa all'andamento della Società;
- i componenti del Collegio Sindacale, nel controllo e nella verifica della correttezza formale e sostanziale dell'attività della Società e del funzionamento del sistema di controllo interno;
- il Direttore Generale ed i Dirigenti, nel dare concretezza alle attività di direzione della Società, nella gestione delle attività interne ed esterne;
- i dipendenti e tutti i collaboratori con cui si intrattengono rapporti contrattuali, a qualsiasi titolo, anche occasionali e/o soltanto temporanei;
- tutti coloro che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con la Società.

5.1. Finalità del Modello

Il Modello predisposto da Liguria Digitale si fonda su un sistema strutturato ed organico di procedure nonché di attività di controllo che:

- individuano le aree/i processi di possibile rischio nell'attività aziendale, vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che siano commessi reati;
- definiscono il sistema normativo interno, finalizzato alla prevenzione dei reati, nel quale sono tra l'altro ricompresi:
  - ✓ il Codice Etico, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali assunti dai

dipendenti, amministratori e collaboratori a vario titolo della Società ed applicabili agli altri destinatari così come dettagliati nel Codice Etico stesso;

- ✓ il sistema di deleghe, poteri di firma e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
- ✓ procedure formalizzate, tese a disciplinare le modalità operative nelle aree a rischio;

- trovano il proprio presupposto in una struttura organizzativa coerente con le attività aziendali, volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una appropriata segregazione delle funzioni, assicurando che gli assetti previsti dalla struttura organizzativa siano realmente attuati, attraverso:
  - o un Organigramma formalmente definito, chiaro ed adeguato all'attività da svolgere;
  - o un sistema di deleghe di attività interne e di procure per rappresentare la Società verso l'esterno che assicuri una chiara e coerente segregazione delle funzioni;
- individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporne l'aggiornamento.

Pertanto il Modello si propone come finalità quelle di:

- migliorare il sistema di Governance;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto di Liguria Digitale nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di Liguria Digitale che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni;
- ribadire che Liguria Digitale non tollera comportamenti illeciti, non rilevando in alcun modo la finalità perseguita ovvero l'erroneo

convincimento di agire nell'interesse o a vantaggio della Società, in quanto tali comportamenti sono comunque contrari ai principi etici cui Liguria Digitale intende attenersi e dunque in contrasto con l'interesse della stessa;

- censurare fattivamente i comportamenti posti in essere in violazione del Modello attraverso la comminazione di sanzioni disciplinari e/o contrattuali.

5.2. Lo sviluppo del Modello

La metodologia adottata, in termini di organizzazione, definizione delle modalità operative, strutturazione in fasi, assegnazione delle responsabilità tra le varie funzioni aziendali, è stata elaborata al fine di garantire la qualità e l'autorevolezza dei risultati.

Il Modello è stato predisposto e mantenuto aggiornato da Liguria Digitale tenendo presenti, come già anticipato, le prescrizioni del Decreto e le Linee Guida elaborate in materia da Confindustria.

Di seguito vengono descritte le fasi nelle quali Liguria Digitale ha articolato il lavoro di individuazione delle aree a rischio e di rilevazione del sistema attuale di presidi e controlli volti a prevenire i reati previsti nel Decreto, mentre la descrizione in dettaglio del processo di trattamento e gestione del rischio di commissione dei reati contemplati dal D.lgs. 231/01 è descritta nel documento "Valutazione dei rischi ex. D.lgs. 231/01".

5.3. Il trattamento del Rischio

Un concetto fondamentale nella costruzione di un sistema di controllo preventivo è quello di "***rischio accettabile***". Nella progettazione di sistemi di controllo a tutela dei rischi di business, definire il rischio accettabile è un'operazione relativamente semplice, almeno dal punto di vista concettuale. Il rischio è ritenuto accettabile quando i controlli aggiuntivi "costano" più della risorsa da proteggere.

Nel caso del Decreto la logica economica dei costi non può però essere un riferimento utilizzabile in via esclusiva. È pertanto importante che ai fini dell'applicazione delle norme del Decreto sia definita una soglia effettiva che consenta di porre un limite alla quantità/qualità delle misure di prevenzione da introdurre per evitare la commissione dei reati considerati.

In assenza di una determinazione del rischio accettabile, la quantità/qualità di controlli preventivi istituibili è infatti virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale.

Riguardo al sistema di controllo preventivo da costruire in relazione al rischio di commissione delle fattispecie di reato contemplate dal Decreto, la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un

sistema di prevenzione tale da non poter essere aggirato se non in modo fraudolento.

Questa soluzione è in linea con la logica della "elusione fraudolenta" del modello organizzativo quale esimente espressa dal citato Decreto ai fini dell'esclusione della responsabilità amministrativa dell'Ente (art. 6, co. 1, lett. c), "le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione".

Diversamente, nei casi di reati di omicidio colposo e lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, la soglia concettuale di accettabilità, agli effetti esimenti del Decreto, è rappresentata dalla realizzazione di una condotta (non accompagnata dalla volontà dell'evento morte/lesioni personali) in violazione del modello organizzativo di prevenzione (e dei sottostanti adempimenti obbligatori prescritti dalle norme prevenzionistiche) nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal Decreto da parte dell'apposito OdV. Ciò in quanto l'elusione fraudolenta dei modelli organizzativi appare incompatibile con l'elemento soggettivo dei reati di omicidio colposo e lesioni personali colpose, di cui agli artt. 589 e 590 del codice penale.

Pertanto, premesso che i modelli organizzativi devono essere idonei a prevenire i reati di origine sia dolosa sia colposa previsti dal Decreto, primo obiettivo per la costruzione di un modello organizzativo è regolare e presidiare le attività che comportano un rischio di reato al fine di evitarne la commissione.
Ciò tenendo presente che, come accennato sopra, gli stessi reati possono comunque essere commessi anche una volta attuato il Modello.
In tal caso, nell'ipotesi di reati dolosi, solo se realmente voluti dall'agente sia come condotta che come evento.

Il Modello e le relative misure devono essere implementate in modo che l'agente non solo debba "volere" l'evento reato (ad esempio corrompere un pubblico funzionario) ma possa attuare il suo proposito criminoso soltanto aggirando fraudolentemente (ad esempio attraverso artifizi e/o raggiri) le indicazioni della Società. L'insieme di misure che l'agente, se vuol delinquere, è costretto a "forzare", deve essere realizzato in relazione alle specifiche attività dell'Ente considerate a rischio ed ai singoli reati ipoteticamente collegabili alle stesse.

Nell'ipotesi, invece, di reati colposi, gli stessi devono essere voluti dall'agente solo come condotta e non anche come evento.

La metodologia per la realizzazione di un sistema di gestione del rischio di seguito esposta ha valenza generale. Il procedimento descritto può essere infatti applicato a varie tipologie di rischio.

5.3.1. Raccolta ed analisi di tutta la documentazione

Liguria Digitale, per pianificare le attività interne di identificazione delle aree a rischio e di rilevazione del sistema di controllo interno correlato, provvede a raccogliere ed esaminare la documentazione di carattere organizzativo-procedurale presente in azienda: procedure, norme organizzative, organigrammi, sistema delle deleghe e delle procure, ordini di servizio, eventuali registrazioni ed evidenze dei processi interni, piani ed evidenze di audit, ecc.

Inoltre ha condotto un'analisi storica dei casi già emersi nel passato relativi a precedenti penali, civili, o amministrativi nei confronti della Società o suoi dipendenti che abbiano punti di contatto con la normativa introdotta dal Decreto.

La raccolta della documentazione della struttura societaria ed organizzativa e l'analisi della stessa da un punto di vista sia tecnico-organizzativo sia legale consente di individuare i processi/attività sensibili ed una preliminare identificazione delle funzioni responsabili di tali processi/attività.

Al termine è stato predisposto un piano di lavoro dettagliato delle fasi successive, suscettibile di revisione in funzione dei risultati raggiunti e delle considerazioni emerse.

5.3.2. Identificazione dei processi e delle attività a rischio

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

In questa fase sono state identificate le aree a rischio potenziale di commissione di reati rilevanti ai sensi del Decreto e/o strumentali intendendosi per tali, rispettivamente, le attività il cui svolgimento potrebbe dare direttamente adito alla commissione di una delle fattispecie di reato contemplate dal Decreto e le aree in cui, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei reati in oggetto.

Sono state effettuate analisi delle varie *policies* e procedure (o prassi), condotte interviste a più soggetti, con diverse e specifiche competenze, al fine di favorire le migliori conoscenze in relazione all'operatività di ciascun singolo settore di attività della Società. I risultati degli incontri, oltre ad illustrare contenuti e modalità operative, hanno consentito di individuare i profili di rischio di commissione delle ipotesi di reato individuate dal Decreto. Per ciascuna attività, si è provveduto, in seguito, ad indicare le specifiche ragioni di sussistenza o insussistenza di ciascun profilo di rischio.

Il risultato di questa fase è la creazione di una mappatura delle attività che, in considerazione degli specifici contenuti, potrebbero essere esposte alla potenziale commissione dei reati richiamati dal Decreto.

5.3.3. Identificazione ed analisi degli attuali presidi al rischio

L'attività è stata condotta attraverso l'organizzazione di incontri specifici con i Responsabili di Liguria Digitale, resi edotti dei contenuti e della portata del Decreto nel corso degli incontri medesimi e la consegna di materiale esplicativo (quando ritenuto necessario), ivi incluso l'elenco descrittivo dei reati introdotti dal Decreto.

I risultati di tale attività (*Risk Assessment*) sono raccolti e formalizzati nella Parte Speciale (e relativi allegati) del presente Modello Organizzativo, utilizzando i dati disponibili (procedure, prassi, documenti, etc.) eventualmente integrati dalle interviste personali con i principali responsabili aziendali.

Le informazioni raccolte hanno anche lo scopo di indicare, per ciascuna di tali attività, il profilo di rischio potenziale e la ragione di sussistenza di tale profilo di rischio (profili di rischio-reato potenziali) e di stabilire le modalità di gestione e gli strumenti di controllo, con particolare attenzione ai controlli preventivi esistenti a presidio dei rischi derivanti.

5.3.4. Gap Analisys

Le informazioni raccolte riassumono, inoltre, con riferimento a ciascun profilo di rischio-reato potenziale, le occasioni, anch'esse potenziali, di commissione dei reati stessi nonché, con riferimento a ciascuna delle principali modalità di loro realizzazione individuate:

- ✓ i meccanismi di controllo rilevati nell'ambito della Funzione/Direzione considerata;
- ✓ l'adeguatezza degli stessi ossia la loro attitudine a prevenire o individuare comportamenti illeciti;
- ✓ i suggerimenti utili a porre rimedio ad eventuali disallineamenti rispetto al Modello a tendere.

Infatti le situazioni di rischio e dei relativi presidi vengono confrontate con le esigenze ed i requisiti imposti dal Decreto, al fine di individuare le eventuali lacune e carenze del sistema esistente. Si è provveduto quindi a richiedere al soggetto responsabile della gestione delle attività a rischio non sufficientemente presidiate, di identificare gli interventi che più efficacemente risultassero idonei a

prevenire in concreto le identificate ipotesi di rischio, tenendo conto anche dell'esistenza di regole operative esplicitamente codificate ovvero non normate, ma ugualmente rispettate nella pratica operativa.

Le interviste, sviluppate attraverso la partecipazione e la collaborazione alle attività sopra richiamate dell'intera struttura organizzativa di Liguria Digitale sono a disposizione dell'OdV ai fini dello svolgimento dell'attività istituzionale ad esso demandata dal Decreto stesso.

5.3.5. Costruzione del sistema di controllo preventivo

Il sistema di controllo preventivo è tale da garantire che i rischi di commissione dei reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un livello "accettabile", secondo la definizione esposta in premessa. Si tratta, in sostanza, di progettare quelli che il Decreto definisce "specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire".

Le componenti di un sistema di controllo interno (preventivo), per le quali esistono consolidati riferimenti metodologici, sono molteplici. E' importante sottolineare come le componenti di controllo indicate debbano integrarsi in un sistema organico, nel quale non tutte necessariamente devono coesistere e dove la possibile debolezza di una componente può essere controbilanciata dal rafforzamento di una o più delle altre componenti in chiave compensativa.

Il sistema di controlli preventivi dovrà essere tale che lo stesso:

- ✓ nel caso di "*reati dolosi*", non possa essere aggirato se non con intenzionalità;
- ✓ nel caso di "*reati colposi*", come tali incompatibili con l'intenzionalità fraudolenta, risulti comunque violato, nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito Organismo.

5.3.6. Complementarietà delle Misure di Prevenzione del Modello con il PTPC

L'attività di trattamento dei rischi individuati dal D.lgs. 231/01 ha sviluppato misure di prevenzione e definito responsabilità correlate, relativamente al contenimento del fenomeno corruttivo, anche tenendo conto di quanto definito e implementato nell'ambito del Piano Triennale di Prevenzione della Corruzione vigente (PTPC).
In tal senso, seppur la scelta della Società è stata quella di tenere distinto il presente Modello dal PTPC, la coerenza tra i due documenti

è garantita sia in termini di finalità, obiettivi, indicatori e risorse associate, sia in termini di modalità e sviluppo dei contenuti.
Sono state infatti implementate sinergie a livello organizzativo e di responsabilità tra l'OdV e il RPCT, nonché a livello documentale e di processo tra i contenuti del Modello e del PTPC.

L'integrazione è evidente ove si considerino gli elementi attinenti la corruzione su cui si fonda il sistema di controllo preventivo adottato da Liguria Digitale: tali elementi devono dare infatti piena attuazione a quanto prescritto dal D.lgs. 231/01 e dalla Legge 190/2012, contestualizzando le diverse disposizioni normative nella realtà organizzativa e funzionale della Società al fine di rendere tale sistema preventivo concreto ed efficace.

5.3.6.1. Definizione dei protocolli e del Modello

I protocolli contengono la disciplina che il soggetto avente la responsabilità operativa ha contribuito ad individuare come la più idonea a governare il profilo di rischio individuato: di fatto sono un insieme di regole originato da una dettagliata analisi di ogni singola attività e del sistema di prevenzione del rischio.

I protocolli sono ispirati alla regola di rendere documentate e verificabili le varie fasi del processo decisionale, onde sia possibile risalire alla motivazione che ha guidato la decisione.

Originati dall'attività di valutazione del sistema di controllo interno, i protocolli con riferimento alle aree a rischio reato e/o strumentali citate intendono fornire le regole di comportamento e le modalità operative e di controllo alle quali Liguria Digitale deve adeguarsi con riferimento all'espletamento delle attività a rischio e/o strumentali.

Pertanto, i citati protocolli consentono di raggiungere i seguenti obiettivi:

- ✓ **segregazione** funzionale delle attività operative e di controllo; in virtù di tale principio, Liguria Digitale articola la propria struttura organizzativa in modo tale da garantire che nessuna funzione aziendale gestisca in autonomia un intero processo; la concreta attuazione di tale principio prevede che l'autorizzazione al compimento di una determinata operazione e le successive fasi di esecuzione e controllo in ordine all'avvenuta esecuzione dell'operazione medesima siano poste sotto la responsabilità di soggetti diversi. Rappresenta una declinazione del principio di segregazione delle funzioni l'utilizzo di sistemi informatici che abilitino allo svolgimento di determinate operazioni solamente alcune persone identificate e specificamente autorizzate, garantendo altresì la protezione delle relative informazioni;
- ✓ **tracciabilità** delle operazioni a rischio e dei controlli posti in essere per impedire la commissione dei reati; in base a tale

principio, ogni operazione aziendale viene adeguatamente documentata, per consentire in ogni momento eventuali controlli in ordine alle caratteristiche e alle motivazioni dell'operazione medesima o per poter risalire ai soggetti che, rispettivamente, l'hanno autorizzata, effettuata, registrata, o ne hanno verificato il corretto svolgimento. La salvaguardia di dati e procedure in ambito informatico è assicurata dall'adozione delle misure di sicurezza previste dal D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) per tutti i trattamenti di dati effettuati con strumenti elettronici;

- ✓ **ripartizione** (**sistema delle procure e deleghe**) ed attribuzione dei poteri autorizzativi e decisionali e delle responsabilità di ciascuna struttura, basate su principi di trasparenza, chiarezza e verificabilità delle operazioni.

  L'individuazione chiara e univoca dei profili aziendali a rischio reato rappresenta un ulteriore strumento organizzativo di prevenzione e contribuisce peraltro a dare attuazione al sopra citato principio di segregazione dei compiti.

  Attraverso il sistema di deleghe e procure Liguria Digitale attribuisce formalmente specifici poteri a soggetti determinati, i quali a loro volta hanno l'obbligo di esercitarli nei limiti entro i quali sono stati loro conferiti. Il sistema è strutturato in modo tale che i poteri autorizzativi e di firma attribuiti siano: coerenti con le responsabilità organizzative e gestionali assegnate e, ove richiesto, circoscritti attraverso l'indicazione dell'importo massimo e della natura delle spese per le quali il procuratore è legittimato ad impegnare la Società; chiaramente definiti e conosciuti all'interno della Società medesima.

  L'assegnazione dei poteri deve avvenire tramite comunicazione formale formulata per iscritto.

  L'atto attributivo di specifiche funzioni deve rispettare i requisiti eventualmente richiesti dalla legge (es. delega in materia di salute e sicurezza dei lavoratori).

I protocolli si completano e si integrano con le regole previste dal Codice Etico che rappresentano, proprio per esser state opportunamente strutturate sulla base delle esigenze espresse dal Decreto, uno strumento fondamentale per esprimere quei principi di deontologia aziendale che la Società riconosce come propri e sui quali fonda una sana, trasparente e corretta gestione delle attività di tutti i dipendenti.

Secondo le indicazioni appena fornite, qui di seguito sono elencate, con distinto riferimento ai **reati dolosi** e **colposi** previsti dal Decreto, quelle che generalmente vengono ritenute le componenti (i

protocolli) di un sistema di controllo preventivo, che dovranno essere attuate a livello aziendale per garantire l'efficacia del Modello.

5.4. Componenti del Modello per Reati Dolosi

Le componenti del Modello per i Reati Dolosi sono:

Codice etico (o di comportamento) con riferimento ai reati considerati

L'adozione di principi etici in relazione ai comportamenti che possono integrare le fattispecie di reato previste dal Decreto costituisce la base su cui impiantare il sistema di controllo preventivo. Tali principi possono essere inseriti in codici etici di carattere più generale, laddove esistenti o invece essere oggetto di autonoma previsione.

Sistema organizzativo

Deve essere sufficientemente formalizzato e chiaro, soprattutto per quanto attiene all'attribuzione di responsabilità, alle linee di dipendenza gerarchica ed alla descrizione dei compiti, con specifica previsione di principi di controllo quali, ad esempio, la contrapposizione di funzioni. Nell'ambito del sistema organizzativo, attenzione andrà prestata ai sistemi di gestione del personale e dei dipendenti. Tali sistemi sono necessari per indirizzare le attività del personale operativo e manageriale verso l'efficiente conseguimento degli obiettivi aziendali.

Prassi o Procedure manuali ed informatiche

L'utilizzo di prassi o procedure tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo (quadrature; approfondimenti informativi su particolari soggetti quali agenti, consulenti, intermediari). Una particolare efficacia preventiva riveste lo strumento di controllo rappresentato dalla separazione di compiti fra coloro che svolgono fasi (attività) cruciali di un processo a rischio. In questo campo, specifico interesse ricopre l'area della gestione finanziaria, dove il controllo procedurale si avvale di strumenti consolidati nella pratica amministrativa, fra cui abbinamento firme, riconciliazioni frequenti, supervisione, separazione di compiti con la già citata contrapposizione di funzioni, ad esempio fra la funzione acquisti e la funzione amministrativa finanziaria e/o di tesoreria.
Particolare attenzione deve essere riposta sui flussi finanziari non rientranti nei processi tipici aziendali, soprattutto se si tratta di ambiti non adeguatamente proceduralizzati e con caratteri di estemporaneità e discrezionalità. In ogni caso è necessario che siano sempre salvaguardati i principi di trasparenza, verificabilità, inerenza all'attività aziendale.

Poteri autorizzativi e di firma

Devono essere assegnati in coerenza con le responsabilità organizzative e gestionali definite e prevedere, se necessario, una indicazione delle soglie di approvazione delle spese.

Sistema di controllo di gestione

Deve essere in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare. Funzionale a questo è la definizione di opportuni indicatori per le singole tipologie di rischio rilevato ed i processi di *Risk assessment* interni alle singole funzioni aziendali.

Comunicazione al personale e sua formazione

Sono due importanti requisiti del Modello ai fini del suo buon funzionamento. Con riferimento alla comunicazione, essa deve riguardare ovviamente il codice etico, ma anche gli altri strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano. La comunicazione deve essere: capillare, efficace, autorevole (cioè emessa da un livello adeguato), chiara e dettagliata, periodicamente ripetuta. Accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione rivolto al personale delle aree a rischio, appropriatamente tarato in funzione dei livelli dei destinatari, che illustri le ragioni di opportunità, oltre che giuridiche, che ispirano le regole e la loro portata concreta.

5.5. Componenti del Modello per Reati Colposi

Fermo restando quanto già precisato in relazione alle fattispecie di reato doloso, valgono le seguenti indicazioni.

Codice etico (o di comportamento) con riferimento ai reati considerati

È espressione anche della politica aziendale per la salute e sicurezza sul lavoro e indica la visione, i valori essenziali e le convinzioni dell'azienda in tale ambito. Serve pertanto a definire la direzione, i principi d'azione ed i risultati a cui tendere nella materia.

Struttura organizzativa

È necessaria una struttura organizzativa con compiti e responsabilità in materia di salute e sicurezza sul lavoro definiti formalmente in coerenza con lo schema organizzativo e funzionale dell'azienda, a partire dal datore di lavoro fino al singolo lavoratore. Particolare attenzione va riservata alle figure specifiche operanti in tale ambito (RSPP - Responsabile del Servizio di Prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC – Medico Competente, addetti primo soccorso, addetto emergenze in caso d'incendio). Devono inoltre essere tenute in considerazione anche le figure specifiche previste da altre normative di riferimento nonché i requisiti e la documentazione relativa a presidio della sicurezza.

Tale impostazione comporta in sostanza che:

- ✓ nella definizione dei compiti organizzativi e operativi della direzione aziendale, dei dirigenti, dei preposti e dei lavoratori siano esplicitati anche quelli relativi alle attività di sicurezza di rispettiva competenza nonché le responsabilità connesse all'esercizio delle stesse attività;
- ✓ siano in particolare documentati i compiti del Responsabile del Servizio di Prevenzione e Protezione e degli eventuali addetti allo stesso servizio, del Rappresentante dei Lavoratori per la Sicurezza, degli addetti alla gestione delle emergenze e del medico competente.

Formazione e addestramento

Sono componenti essenziali per la funzionalità del Modello. Lo svolgimento di compiti che possono influenzare la salute e sicurezza sul lavoro richiede una adeguata competenza, da verificare ed alimentare attraverso la somministrazione di formazione e addestramento finalizzati ad assicurare che tutto il personale, ad ogni livello, sia consapevole della importanza della conformità delle proprie azioni rispetto al modello organizzativo e delle possibili conseguenze dovute a comportamenti che si discostino dalle regole dettate dal Modello.

In concreto, ciascun lavoratore/operatore aziendale deve ricevere una formazione sufficiente ed adeguata con particolare riferimento al proprio posto di lavoro ed alle proprie mansioni. Questa deve avvenire in occasione dell'assunzione, del trasferimento o cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie, di nuove sostanze e preparati pericolosi.

Comunicazione e coinvolgimento

La circolazione delle informazioni all'interno dell'azienda assume un valore rilevante per favorire il coinvolgimento di tutti i soggetti interessati e consentire consapevolezza ed impegno adeguati a tutti livelli.

Il coinvolgimento dovrebbe essere realizzato attraverso:

- ✓ la consultazione preventiva in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
- ✓ riunioni periodiche che tengano conto almeno delle richieste fissate dalla legislazione vigente utilizzando anche le riunioni previste per la gestione aziendale.

Gestione operativa

Il sistema di controllo, relativamente ai rischi per la salute e sicurezza sul lavoro dovrebbe integrarsi ed essere congruente con la gestione complessiva dei processi aziendali.

Dalla analisi dei processi aziendali e delle loro interrelazione e dai risultati della valutazione dei rischi deriva la definizione delle modalità per lo

svolgimento in sicurezza delle attività che impattano in modo significativo sulla salute e sicurezza sul lavoro. L'azienda identifica le aree di intervento associate agli aspetti di salute e sicurezza ed esercita una gestione operativa regolata.

In questo senso, particolare attenzione dovrebbe essere posta riguardo a:

- ✓ assunzione e qualificazione del personale;
- ✓ organizzazione del lavoro e delle postazioni di lavoro;
- ✓ acquisizione di beni e servizi impiegati dall'azienda e comunicazione delle opportune informazioni a fornitori ed appaltatori;
- ✓ manutenzione normale e straordinaria, nonché la gestione di eventuali relativi cantieri;;
- ✓ qualificazione e scelta dei fornitori e degli appaltatori;
- ✓ gestione delle emergenze;
- ✓ procedure per affrontare le difformità rispetto agli obiettivi fissati ed alle regole del sistema di controllo.

Sistema di monitoraggio della sicurezza

La gestione della salute e sicurezza sul lavoro dovrebbe prevedere una fase di verifica del mantenimento delle misure di prevenzione e protezione dei rischi adottate e valutate idonee ed efficaci. Le misure tecniche, organizzative e procedurali di prevenzione e protezione realizzate dall'azienda dovrebbero essere sottoposte a monitoraggio pianificato.

L'impostazione di un piano di monitoraggio si dovrebbe sviluppare attraverso:

- ✓ programmazione temporale delle verifiche (frequenza);
- ✓ attribuzione di compiti e di responsabilità esecutive;
- ✓ descrizione delle metodologie da seguire;
- ✓ modalità di segnalazione delle eventuali situazioni difformi.

5.6. I principi di controllo

Le componenti dei Modelli organizzativi sopra descritte devono integrarsi in un'architettura del sistema che rispetti una serie di principi di controllo, fra cui:

"Ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua".

Per ogni operazione vi deve essere un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

La salvaguardia di dati e procedure in ambito informatico può essere assicurata mediante l'adozione delle misure di sicurezza già previste dal D.lgs. 196/2003 (Codice in materia di protezione dei dati personali) per tutti i trattamenti di dati effettuati con strumenti elettronici.

L'art. 31 del Codice, infatti, prescrive l'adozione di misure di sicurezza tali da ridurre al minimo "i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

"*Nessuno può gestire in autonomia un intero processo*"

Il sistema deve garantire l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione.

Inoltre, occorre che:

- ✓ a nessuno vengano attribuiti poteri illimitati;
- ✓ i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione;
- ✓ i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate.

"Documentazione dei controlli".

Il sistema di controllo dovrebbe documentare (eventualmente attraverso la redazione di verbali, di rapporti di audit) l'effettuazione dei controlli di conformità e di *compliance* alle disposizioni di legge, ad eventuali regolamenti vigenti, alle regole ed alle disposizioni interne fissate dalla Società stessa.

5.7. Il Sistema delle Responsabilità

I sistemi gestionali presenti in Liguria Digitale risultano fondati su:

- ✓ un sistema di procure/deleghe attribuite ai livelli aziendali più alti;
- ✓ un sistema di prassi e/o procedure che regolamentano i processi e le attività aziendali;
- ✓ una organizzazione aziendale basata sul principio della separazioni dei compiti.

I requisiti essenziali del sistema di attribuzione delle deleghe, ai fini di una efficace prevenzione dei reati previsti dal Decreto, sono i seguenti:

- ✓ tutti coloro che intrattengono per conto di Liguria Digitale rapporti con la PA ed in genere con i terzi devono essere dotati di formale delega scritta in tal senso; ove la delega abbia ad oggetto compiti o funzioni

permanenti dovrà essere resa nota ai terzi mediante adeguate procedure di pubblicità legale;

- ✓ le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- ✓ il conferimento di funzioni deve rispondere a criteri di effettività e integralità; le funzioni delegate dovranno essere svolte senza ingerenze da parte del delegante con l'avvertenza che la doverosa attività di controllo del delegante stesso non dovrà mai essere considerata attività di ingerenza;
- ✓ una procedura ad hoc deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, ecc.).

5.8. Struttura del documento

Il presente documento (Modello) è costituito da una "Parte Generale" e dalle "Parti Speciali A, B, C, D, E ed F", predisposte per approfondire le diverse tipologie di reato considerate come possibile rischio per Liguria Digitale.

Nella "Parte Generale", dopo un richiamo ai principi del Decreto, vengono illustrate le componenti essenziali del Modello con particolare riferimento all'OdV, alla formazione del personale e alla diffusione del Modello nel contesto aziendale ed extra-aziendale e al Sistema Disciplinare.

La Parte Speciale "A" è relativa alle tipologie specifiche di reati previste ai sensi degli articoli 24, 25 e 25-decies del Decreto, ossia per i reati realizzabili in danno della Pubblica Amministrazione o dell'Amministrazione della Giustizia.

La Parte Speciale "B" è relativa alle tipologie specifiche di reati previste ai sensi dell'art. 25-ter del Decreto, cioè per i c.d. "Reati societari".

La Parte Speciale "C" è relativa alle tipologie specifiche di reati previste ai sensi dell'articolo 25-septies del Decreto, ossia i reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene, della sicurezza e della salute sul lavoro.

Nella Parte Speciale "D" sono descritti i delitti informatici e quelli relativi al trattamento illecito dei dati, oggi rilevanti ai sensi del Decreto in virtù di quanto previsto dall'art. 24-bis con indicazione delle relative aree di rischio e dei presidi di ordine generale ad esse preposti.

La Parte Speciale "E" è relativa ai delitti in materia di violazione del diritto d'autore previsti dall'art. 25-novies.

La Parte Speciale "F" è dedicata all'esame dei reati ambientali rilevanti ai sensi del Decreto in quanto previsti dall'art. 25-undecies, con indicazione delle relative aree di rischio e dei presidi di ordine generale ad esse preposti.

Con riferimento agli altri "reati presupposto" della responsabilità amministrativa dell'ente ai sensi del Decreto, quali:

- i falsi nummari (art. 25-bis),
- i delitti contro la personalità individuale (art. 25-quinquies),
- i delitti con finalità di terrorismo o di eversione dell'ordinamento democratico (art. 25-quater),
- i reati per pratiche di mutilazione degli organi genitali femminili (art. 25-quater 1),
- i reati transnazionali (art. 10 L. 146/06),
- i delitti di criminalità organizzata (art. 24-ter),
- i delitti di ricettazione, riciclaggio e impiego di beni di illecita provenienza (art. 25-octies),
- i delitti contro l'industria e il commercio (art. 25-bis 1),
- i reati di abuso di mercato (art. 25-sexies),
- il reato di impiego di cittadini di paesi terzi il cui soggiorno in Italia è irregolare (art. 25-duodecies),

si è ritenuto che il rischio effettivo di concretizzazione di comportamenti che possano configurare i suddetti reati sia trascurabile. Infatti le procedure generali di gestione aziendale e i protocolli, come il Codice Etico ed i regolamenti interni, presidiano in modo completo le suddette aree.

Qualora si rendesse necessario procedere all'emanazione di ulteriori Parti Speciali, relativamente a nuove fattispecie di reato attinenti alle aree di business della Società, è demandato all'Organo Amministrativo il potere di integrare il presente Modello.

Costituiscono inoltre parte integrante del Modello il PTPC ed il Codice Etico, nel quale sono espressi i principi generali ed i valori cui deve essere ispirata l'attività di tutti coloro che, a qualsiasi titolo, operano in nome e per conto di Liguria Digitale.

5.9. Adozione e criteri di aggiornamento del Modello

L'art. 6, comma 1, lettera a) del Decreto richiede che il Modello sia un "atto di emanazione dell'organo dirigente".

L'adozione dello stesso e le successive modifiche e integrazioni sono di competenza dell'Amministratore Unico di Liguria Digitale (anche su proposta dell'OdV) che provvede mediante determina.

La versione più aggiornata del Modello è immediatamente resa disponibile all'OdV.

L'indice delle revisioni, indicato nel documento, garantisce la tracciabilità del Modello e consente di rappresentare la sua evoluzione temporale e sostanziale.

Nella prassi, l'aggiornamento del Modello previe modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- significative violazioni delle prescrizioni del Modello;
- modificazioni dell'assetto interno di Liguria Digitale e/o delle modalità di svolgimento delle attività d'impresa;
- modifiche normative;
- risultanze dei controlli;
- accertamento di gravi fatti penalmente rilevanti commessi anche anteriormente all'approvazione del Modello.

Una volta approvate, le modifiche e le istruzioni per la loro immediata applicazione sono comunicate all'OdV, il quale, a sua volta, provvederà, senza indugio, a rendere le stesse modifiche operative e a curare la corretta comunicazione dei contenuti all'interno e all'esterno di Liguria Digitale.
L'OdV provvederà, altresì, mediante apposita relazione, ad informare l'Amministratore Unico circa l'esito dell'attività intrapresa in ottemperanza alla delibera che dispone l'aggiornamento e/o adeguamento del Modello.
L'OdV mantiene, in ogni caso, precisi compiti e poteri in merito alla cura, sviluppo e promozione del costante aggiornamento del Modello. A tal fine, formula osservazioni e proposte, attinenti l'organizzazione ed il sistema di controllo, alle strutture aziendali a ciò preposte o, in casi di particolare rilevanza, all'Amministratore Unico.
In particolare, al fine di garantire che le variazioni del Modello siano operate con la necessaria tempestività ed efficacia, senza al contempo incorrere in difetti di coordinamento tra i processi operativi, le prescrizioni contenute nel Modello e la diffusione delle stesse, l'Amministratore Unico ha il compito di apportare con cadenza periodica le modifiche al Modello che attengano ad aspetti di carattere descrittivo. Si precisa che con l'espressione "aspetti di carattere descrittivo" si fa riferimento ad elementi ed informazioni che derivano da atti deliberati dagli Organi di Liguria Digitale (come ad esempio modifica statutaria, ecc.) o da funzioni aziendali munite di specifica delega (come ad esempio la ridefinizione dell'organigramma, ecc.).
Il Modello sarà, in ogni caso, sottoposto a procedimento di revisione periodica almeno con cadenza triennale da disporsi mediante determina dell'Amministratore Unico.

6. ORGANISMO DI VIGILANZA

Gli artt. 6 e 7 del D.lgs. n. 231/01 prevedono che sia istituito un OdV incaricato di vigilare sul corretto funzionamento, l'efficacia e l'osservanza del modello di organizzazione e gestione.

Considerato il disposto dell'art. 6 del Decreto, nonché le più significative pronunce giurisprudenziali intervenute sul tema, l'Amministratore Unico della società ritiene che l'OdV di Liguria Digitale possa avere una struttura collegiale anche mista e possa quindi essere composto sia da membri interni sia esterni.

A garanzia del principio di terzietà, l'OdV è collocato in posizione gerarchica di vertice della Società, riportando e rispondendo direttamente all'Amministratore Unico ed al Collegio Sindacale.

L'OdV opera secondo modalità e termini indicati nello "Statuto dell'OdV", in allegato al presente Modello, e nel "Regolamento dell'Organismo di Vigilanza" di Liguria Digitale.

L'attività dell'OdV è regolamentata sulla base di due documenti collegati ed autonomi:

- lo *Statuto dell'OdV*, formalmente approvato dall'organo amministrativo, che fissa le regole generali e di relazione trasparente con le parti interessate;
- il *Regolamento dell'OdV*, strumento operativo che l'Organismo stesso adotta in funzione del principio di autonomia di cui gode.

6.1. Struttura e composizione dell'Organismo di Vigilanza

L'OdV è un organo collegiale composto da almeno tre componenti, interni ed esterni (questi ultimi intesi come soggetti che non hanno rapporto contrattuale di lavoro subordinato o equivalente con la società), nominati dall'Amministratore Unico. Uno dei membri assume la funzione di Presidente dell'organismo, incaricandosi del coordinamento delle attività.

Affinché l'OdV possa svolgere le attività sulla base delle indicazioni contenute negli artt. 6 e 7 del D.lgs. 231/01, devono essere rispettati i principi di:

a) Autonomia e indipendenza;

b) Professionalità;

c) Continuità d'azione.

Tali requisiti possono essere così sintetizzati:

Requisito	Che cosa significa
AUTONOMIA E INDIPENDENZA	Evitare che all'OdV complessivamente inteso siano affidati compiti operativi. Non deve esserci identità tra controllato e controllante. Eliminare ingerenze e condizionamenti di tipo economico o personale da parte degli organi di vertice. Prevedere nel Modello cause effettive di ineleggibilità e decadenza dal ruolo di membri dell'OdV, che garantiscano onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.
PROFESSIONALITÀ	Nominare soggetti competenti in materia ispettiva e consulenziale, in grado di compiere attività di campionamento statistico, di analisi, valutazione e contenimento dei rischi, di elaborazione e valutazione dei questionari. È opportuno che almeno taluno tra i membri dell'OdV abbia competenze giuridiche.
CONTINUITÀ	Predisporre una struttura dedicata all'attività di vigilanza sul Modello. Curare la documentazione dell'attività svolta.

Sul piano soggettivo, i membri dell'organismo devono rispettare i requisiti di professionalità e onorabilità, garantendo, nel contempo, l'assenza di ogni posizione di conflitto (a titolo esemplificativo: relazioni di parentela con gli organi sociali o con il vertice, conflitti di interessi).

Tali soggetti, in virtù dell'attività che sono chiamati a svolgere, devono inoltre essere dotati di adeguate conoscenze di carattere aziendalistico, legale (societario, penale, civile, procedurale, amministrativo) contabile, gestionale.

Al fine del corretto adempimento delle proprie funzioni, di carattere multidisciplinare, l'OdV potrà avvalersi della collaborazione di particolari professionalità, da reperirsi anche all'esterno della Società, capaci di fornire un utile supporto tecnico e specialistico.

6.2. Compiti dell'Organismo di Vigilanza

L'OdV è dotato di autonomi poteri di iniziativa e di controllo.

Ad esso è affidato, in particolare, il compito di vigilare affinché il Modello sia:

a) adeguato ed efficace, ossia idoneo a prevenire la commissione dei reati in relazione alla struttura della Società;

b) effettivo, ossia divulgato ed efficacemente osservato ed attuato da parte dei dipendenti, degli Organi Sociali, dei consulenti e degli altri soggetti a cui il Modello si indirizza;

c) aggiornato, ossia sempre coerente con l'assetto della Società e con le normative sopravvenute.

6.3. Flussi informativi verso l'Organismo di Vigilanza

Al fine di poter esercitare al meglio le proprie funzioni l'OdV è destinatario di qualsiasi informazione, documentazione, segnalazione attinente l'attuazione ed il rispetto del Modello che possa essere utile alla prevenzione dei reati presupposto indicati nel Decreto.

L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto, nonché allo scopo di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo nel corso delle sue verifiche.

L'OdV provvede dunque a stabilire i più appropriati canali di comunicazione attraverso cui gli interlocutori della Società sono tenuti ad inoltrare le proprie segnalazioni circa una sospetta violazione del Modello, una situazione che possa evolvere verso la commissione di uno dei reati presupposto ovvero i propri suggerimenti circa un possibile miglioramento del Modello.

Si rinvia allo "Statuto dell'OdV" per quanto non ulteriormente specificato.

7. IL SISTEMA DI GESTIONE DELLE SEGNALAZIONI O *WHISTLEBLOWING*

In un'ottica di ascolto e miglioramento continuo, Liguria Digitale ha adottato un sistema di segnalazioni delle violazioni a disposizione di chiunque ritenga di segnalare situazioni che possano arrecare danno o pregiudizio alla Società.

A tal fine la Società ha adottato, in ottemperanza alla Legge n. 179/2017 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", un "Sistema interno di segnalazione delle violazioni" (o "Sistema di whistleblowing"):

- finalizzato a far emergere, individuare e combattere eventuali fenomeni corruttivi o comunque illeciti, per tutelare l'azionariato da danni economici e all'immagine, per diffondere la cultura dell'etica, della legalità e della trasparenza all'interno della Società;
- accessibile con qualsiasi dispositivo al link https://liguriadigitale.azurewebsites.net oltre che dalla intranet aziendale;
- basato su protocollo di crittografia che garantisce una rafforzata tutela della riservatezza dell'identità del segnalante che resta anonima in ogni fase del processo e che permette allo stesso di dialogare in modo spersonalizzato e rapido con la Società.

Si tratta di uno strumento utile per trasmettere, in modalità riservata, informazioni riguardanti fatti illeciti che costituiscono:

1) reati a norma della Legge n. 190/2012 (c.d. Legge anticorruzione);

2) reati a norma del D.Lgs. n. 231/2001;

3) abuso di potere per ottenere vantaggi privati;

4) violazioni del Codice Etico o di altre disposizioni aziendali sanzionabili in via disciplinare.

Tale Sistema di Segnalazione Web, regolamentato attraverso specifica Policy, è per Liguria Digitale il canale preferenziale di whistleblowing. Resta inteso che verranno tenute in considerazione anche quelle segnalazioni pervenute al di fuori di tale Sistema, attraverso l'utilizzo dei seguenti indirizzi e-mail:

- anticorruzione@liguriadigitale.it
- odv231@liguriadigitale.it.

In tali casi il RPCT e l'ODV231 si danno reciproca comunicazione delle segnalazioni singolarmente ricevute.

Si precisa infine che anche Committenti, Consulenti, Fornitori e Partner, in relazione all'attività svolta con Liguria Digitale, possono inviare eventuali segnalazioni mediante l'utilizzo dei canali precedentemente esposti.

8. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE E ALL'ESTERNO

8.1. Formazione del personale

La formazione è considerata uno degli elementi maggiormente incisivi al fine di favorire la diffusione della conoscenza del Decreto e delle procedure da adottare per adempiere alle previsioni del Modello ex D.lgs.231/01, nonché una delle principali modalità per dare efficace attuazione al Modello stesso.
Liguria Digitale promuove la conoscenza del Modello, del sistema normativo interno e relativi aggiornamenti tra tutti i dipendenti, che sono pertanto tenuti a conoscerne il contenuto, osservarlo e contribuire alla sua attuazione.
La struttura Human Resources, collaborando con l'OdV, gestisce la formazione del personale sui contenuti del Decreto e sull'attuazione del Modello.
In tale contesto, le azioni comunicative e formative prevedono:

- la pubblicazione del Modello, del PTPC e del Codice Etico sulla *Intranet* aziendale e nelle sezioni dedicate del sito Internet della Società affinché tutti i dipendenti e tutti i collaboratori della Società possano prenderne visione, rispettando i principi in esso contenuti;
- disponibilità del Codice Etico per tutto il personale in forza e distribuzione ai nuovi assunti al momento dell'inserimento in azienda con firma attestante l'avvenuta ricezione e l'impegno alla conoscenza e rispetto delle relative prescrizioni;
- la disponibilità di un corso *on-line* presso la Intranet aziendale sui contenuti del Decreto, del Modello Organizzativo e del Codice Etico (la partecipazione ai programmi formativi è documentata);
- notifiche di aggiornamento sulle modifiche apportate al Modello o al Codice Etico, conseguenti ad intervenute modifiche normative e/o organizzative rilevanti ai fini del Decreto, consultabili sulla Intranet aziendale.

La partecipazione alle sessioni di formazione, così come al corso on-line, è obbligatoria e viene monitorata. Eventuali sessioni formative di aggiornamento, oltre a specifici approfondimenti sul tema a beneficio dei neoassunti nell'ambito del processo di inserimento nell'azienda, saranno effettuate in caso di significative modifiche apportate al Modello, al Codice Etico o relative a sopravvenute normative rilevanti per l'attività della Società, ove l'OdV non ritenga sufficiente, in ragione della complessità della tematica, la semplice diffusione della modifica con le modalità sopra descritte.

8.2. Informativa a collaboratori esterni e partners

Liguria Digitale promuove la conoscenza e l'osservanza del Modello (Parte Generale), del PTPC e del Codice Etico anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori della Società.
L'informativa avviene, per i soggetti sopra elencati, mediante la diffusione di una comunicazione ufficiale sull'adozione dei predetti documenti con invito alla consultazione sul sito Internet della Società.
Liguria Digitale provvede ad inserire nei contratti con controparti commerciali, finanziarie e consulenti apposite clausole contrattuali che prevedono, in caso di inosservanza dei principi etici stabiliti, la possibile risoluzione degli obblighi negoziali.

9. SISTEMA DISCIPLINARE

9.1. Principi generali

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello e nel Codice Etico è condizione essenziale per assicurare l'effettività del Modello stesso.

Al riguardo, infatti, l'articolo 6 comma 2, lettera e) del Decreto prevede che i modelli di organizzazione e gestione debbano "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello".

Ai fini del presente sistema disciplinare, e nel rispetto delle previsioni di cui alla contrattazione collettiva, laddove applicabili, costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del Modello e del Codice Etico adottato da Liguria Digitale. Essendo il Modello costituito anche dal complesso del corpo normativo che ne è parte integrante, ne deriva che per "violazione del Modello" deve intendersi anche la violazione di una o più procedure/protocolli.

L'applicazione delle sanzioni disciplinari prescinde dall'avvio e/o dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello e nel Codice Etico sono assunte da Liguria Digitale in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

L'individuazione e l'applicazione delle sanzioni deve tener conto dei principi di proporzionalità e adeguatezza rispetto alla violazione contestata. A tale proposito, assumono rilievo le seguenti circostanze:

- tipologia dell'illecito contestato;
- circostanze concrete in cui si è realizzato l'illecito;
- modalità di commissione della condotta;
- gravità della violazione, anche tenendo conto dell'atteggiamento soggettivo dell'agente;
- eventuale commissione di più violazioni nell'ambito della medesima condotta;
- eventuale concorso di più soggetti nella commissione della violazione;
- eventuale recidività dell'autore.

Il Sistema Disciplinare viene monitorato dall'OdV e dalla struttura Human Resources.

9.2. I soggetti passibili di sanzioni

Sono indicati i soggetti passibili delle sanzioni previste, suddivisi in differenti categorie:

1) Impiegati e Quadri;
2) Dirigenti e altri soggetti in posizione apicale;
3) Collaboratori, consulenti, partner, controparti ed altri soggetti esterni.

9.3. Le possibili violazioni

Sono indicate le violazioni disciplinarmente rilevanti catalogate in cinque diverse categorie secondo un ordine crescente di gravità:

- Violazione di procedure interne della Società o di procedure/protocolli previsti dal Modello (ad esempio non osservanza delle procedure prescritte, omissione di comunicazioni all'OdV in merito a informazioni prescritte, omissione di controlli, ecc.) o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle procedure o alle istruzioni operative della Società o alle prescrizioni del Modello o del Codice Etico;
- Violazione di procedure interne della Società o di procedure/protocolli previsti dal Modello o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle procedure o alle istruzioni operative della Società o alle prescrizioni del Modello stesso o del Codice Etico che espongano la Società a una situazione oggettiva di rischio di commissione di uno dei Reati previsti dal Decreto;
- Adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle procedure o alle istruzioni operative della Società o alle prescrizioni del presente Modello o del Codice Etico e diretti in modo univoco al compimento di uno o più Reati previsti dal Decreto;
- Adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti palesemente in violazione delle procedure o alle istruzioni operative della Società o delle prescrizioni del presente Modello o del Codice Etico, tale da determinare la concreta applicazione a carico della Società di sanzioni previste dal D.lgs. n. 231/2001;
- Commissione di uno dei Reati previsti dal Decreto.

Si segnala in particolare che la violazione degli obblighi d'informazione verso l'OdV è considerata *illecito disciplinare* e può quindi essere sanzionata.

Sono inoltre indicate le violazioni in materia di **salute e sicurezza sul lavoro** disciplinarmente rilevanti, catalogate in quattro diverse categorie secondo un ordine crescente di gravità, relativamente al mancato rispetto del Modello, qualora la violazione determini:

1. una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione, e sempre che non ricorra una delle condizioni previste nei successivi punti 2, 3 e 4;
2. una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione, e sempre che non ricorra una delle condizioni previste nei successivi punti 3 e 4;
3. una lesione, qualificabile come "grave" ai sensi dell'art. 583, comma 1, c.p., all'integrità fisica di una o più persone, incluso l'autore della violazione, e sempre che non ricorra una delle condizioni previste nel successivo punto 4;
4. una lesione, qualificabile come "gravissima" ai sensi dell'art. 583, comma 1, c.p., all'integrità fisica ovvero la morte di una o più persone, incluso l'autore della violazione.

9.4. Il procedimento di applicazione delle sanzioni

Il procedimento di irrogazione delle sanzioni conseguenti alla violazione del Modello, del Codice Etico e delle procedure/protocolli si differenzia con riguardo a ciascuna categoria di soggetti destinatari quanto alla fase di:

- contestazione della violazione all'interessato;
- determinazione e successiva irrogazione della sanzione.

Il procedimento di irrogazione della sanzione ha, in ogni caso, inizio a seguito della ricezione, da parte degli organi aziendali di volta in volta competenti e di seguito indicati, della comunicazione con cui l'OdV segnala l'avvenuta violazione del Modello.

Più precisamente, in tutti i casi in cui l'OdV riceva una segnalazione ovvero acquisisca, nel corso della propria attività di vigilanza e di verifica, gli elementi idonei a configurare il pericolo di una violazione del Modello, ha l'obbligo di attivarsi al fine di espletare gli accertamenti ed i controlli rientranti nell'ambito della propria attività.

Esaurita l'attività di verifica e di controllo, l'OdV valuta, sulla base degli elementi in proprio possesso, la sussistenza delle condizioni per l'attivazione del procedimento disciplinare, provvedendo ad informare la Direzione e la struttura Human Resources, anche ai fini della valutazione della eventuale rilevanza della condotta rispetto alle altre leggi o regolamenti applicabili.

L'attivazione del procedimento disciplinare resta di competenza esclusiva del vertice aziendale, di concerto con la struttura Human Resources.

9.5. Sanzioni previste e categorie di destinatari

Sono indicate, con riguardo a ognuna delle condotte rilevanti, le sanzioni astrattamente comminabili per ciascuna categoria di destinatari.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal D.lgs. n. 231/2001.

In ogni caso le sanzioni e l'eventuale richiesta di risarcimento dei danni sono commisurate al livello di responsabilità e autonomia del destinatario, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta, ai sensi e per gli effetti del D.lgs. n. 231/2001, a seguito della condotta censurata.

9.5.1. Misure nei confronti di Impiegati e Quadri

La violazione da parte di impiegati e Quadri, soggetti ai CCNL applicati dalla Società, delle singole regole comportamentali di cui al presente Modello e del Codice Etico costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori, nel rispetto delle procedure previste dall'art.7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili, sono quelli previsti dall'apparato sanzionatorio di cui ai CCNL, e precisamente:

- Richiamo verbale;
- Ammonizione scritta;
- Multa;
- Sospensione;
- Licenziamento per mancanze.

Restano ferme, e s'intendono qui richiamate, tutte le previsioni in materia di cui ai CCNL, tra cui:

- L'obbligo, nei casi previsti dai CCNL, della previa contestazione dell'addebito al dipendente e dell'ascolto di quest'ultimo in ordine alla sua difesa;
- L'obbligo, salvo nei casi previsti dai CCNL, che la contestazione sia fatta per iscritto e che il provvedimento non sia emanato se non decorso il numero di giorni, previsti nei CCNL, dalla contestazione dell'addebito (nel corso dei quali il dipendente potrà presentare le sue giustificazioni);

- L'obbligo di motivare al dipendente e comunicare per iscritto la comminazione del provvedimento.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti delle rispettive competenze, al management aziendale.

9.5.2. Misure nei confronti di Dirigenti e altri soggetti in posizione apicale

In caso di violazione, da parte di dirigenti o altri soggetti in posizione apicale, delle procedure previste dal presente Modello o di adozione, nell'espletamento di attività connesse con i Processi Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso o del Codice Etico, la Società applica nei confronti dei responsabili le misure più idonee, anche in conformità a quanto previsto dalla normativa vigente, dal CCNL e dallo Statuto dei Lavoratori.

9.5.3. Misure nei confronti di Collaboratori, consulenti, partner, controparti ed altri soggetti esterni

Ogni violazione da parte di collaboratori, revisori, consulenti, partner, controparti ed altri soggetti esterni delle regole di cui al presente Modello o del Codice Etico agli stessi applicabili o di commissione dei Reati previsti dal Decreto è sanzionata secondo quanto previsto dalla normativa vigente e nelle specifiche clausole contrattuali inserite nei relativi contratti.