MODELLO ORGANIZZATIVO DI GESTIONE E CONTROLLO MODELLO 231

PARTE GENERALE

Redazione	Verifica	Approvazione
Organismo di Vigilanza	Ufficio Affari Legali e Fiscali	Consiglio di Amministrazione

Revisione	Oggetto Modifica	Data
2.0	Emissione del modello ex D. Lgs. n. 231/2001 – Parte Generale e Parte Speciale	

Sommario

1. PREMESSA

Il Decreto Legislativo 8 Giugno 2001, n. 231, ("Decreto") ha introdotto nel nostro ordinamento la disciplina della responsabilità amministrativa da reato delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica.

Ai sensi del Decreto, nel caso in cui vengano commessi i reati presupposto ivi previsti, la Società (in quanto tale) può essere ritenuta responsabile a livello amministrativo, a meno che non dimostri di avere adottato un Modello Organizzativo di Gestione e Controllo ("MOG", "Modello" o "Modello Organizzativo") concretamente idoneo a prevenire la commissione di reati quale quello verificatosi, di talché il reato sia stato commesso eludendo fraudolentemente il Modello in violazione delle disposizioni aziendali.

INFORDATA S.p.a. ("Infordata" o "*la Società*") è società del Gruppo Digital Value, impresa primaria del settore di Technology and Service Solutions, attiva nel settore Large Account, ha adottato il presente Modello Organizzativo con delibera del Consiglio di amministrazione.

Scopo dell'adozione del Modello da parte di Infordata è quello di prevenire e/o mitigare il rischio di commissione dei reati di cui al su richiamato D.Lgs. n. 231/2001. Tale Modello, difatti, testimonia la politica preventivo-organizzativa adottata da Infordata volta a contrastare potenziali fenomeni delittuosi che, in astratto, potrebbero essere consumati nel perseguimento dello scopo sociale e derivanti da condotte poste in essere da coloro i quali a vario titolo, operano in nome, per conto e/o nell'interesse della suddetta Società.

Infordata confida sull'integrità del comportamento di tutti i soggetti (Apicali e Dipendenti) che a vario titolo operano in nome, per conto e/o nell'interesse della Società per mantenere un idoneo livello di applicazione delle disposizioni previste dal presente Modello Organizzativo.

Conseguentemente, il mancato rispetto (in tutto o in parte) delle disposizioni ivi definite (e delle altre disposizioni correlate), sarà considerato come un abuso della fiducia riposta nei confronti dei soggetti che non rispettano le direttive aziendali, con la pedissequa applicazione di idonee sanzioni disciplinari.

2. DEFINIZIONI

Ai fini della presente modello valgono le seguenti definizioni:

a. **Decreto**: Decreto Legislativo 8 giugno 2001, n. 231, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001 e successive modifiche ed integrazioni.

b. **Destinatari**: Soggetti a cui è rivolto il Modello Organizzativo, più precisamente: amministratori, dipendenti, collaboratori e consulenti di Infordata nei limiti di quanto indicato nell'art. 5 del Decreto.

c. **Ente**: Persona giuridica, società o associazione anche priva di personalità giuridica.

d. **Incaricato di pubblico servizio**: Si intende un soggetto che, pur svolgendo un'attività pertinente allo Stato o ad un altro Ente pubblico, ovvero un'attività che pur non immediatamente imputabile ad un soggetto pubblico realizzi direttamente finalità di interesse pubblico, non è dotato dei poteri tipici del pubblico ufficiale e non svolge tuttavia funzioni meramente materiali.

e. **Istituzioni pubbliche**: Si intende, a titolo esemplificativo e non esaustivo: le amministrazioni dello Stato (Amministrazione Finanziaria, Autorità garanti e di Vigilanza, Autorità Giudiziarie, ecc.), le aziende ed amministrazioni dello Stato, le regioni, le

province, i comuni, e loro consorzi e associazioni, le istituzioni universitarie, le camere di commercio, industria, artigianato e agricoltura, gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del servizio sanitario nazionale. La funzione pubblica viene rivestita anche dai membri della Commissione dell'Unione Europea, del Parlamento Europeo, della Corte di Giustizia e della Corte dei Conti Europea, dei funzionari e degli agenti assunti a contratto a norma dello statuto dei funzionari dell'Unione Europea.

f. Modello Organizzativo di Gestione e di Controllo (Modello o Modello Organizzativo): Complesso organico di principi, regole, disposizioni, schemi organizzativi e connessi compiti e responsabilità volto a prevenire i reati e gli illeciti amministrativi, così come previsto dagli articoli 6 e 7 del Decreto, ad integrazione degli strumenti organizzativi e di controllo vigenti in Infordata (Codice Etico, Procedure Operative, Organigrammi, Procure, Deleghe). Il Modello Organizzativo prevede, inoltre, l'individuazione dell'Organismo di Vigilanza e di Controllo e la definizione del sistema sanzionatorio.

g. Organismo di Vigilanza e di Controllo (Organismo di Vigilanza): Organo interno, previsto dall'art. 6 del Decreto, con il compito di vigilare sul funzionamento e sull'osservanza del Modello Organizzativo, nonché di curarne l'aggiornamento.

h. Processi/Aree a rischio/Aree sensibili: Attività aziendali o fasi delle stesse il cui svolgimento potrebbe dare occasione a comportamenti illeciti (reati o illeciti amministrativi) di cui al Decreto.

i. Protocollo: Specifica procedura (principi di comportamento, modalità operative, flussi informativi, ecc.) per la prevenzione dei reati e degli illeciti amministrativi e per l'individuazione dei soggetti coinvolti nelle fasi a rischio dei processi aziendali.

j. Pubblica Amministrazione: Si intendono le istituzioni pubbliche, i pubblici ufficiali e gli incaricati di pubblico servizio.

k. **Pubblico ufficiale**: Si intende un soggetto, pubblico dipendente o privato, che concorre a formare o forma la volontà dell'Ente Pubblico ovvero lo rappresenta all'esterno; un soggetto munito di poteri autorizzativi e di certificazione.

l. **Quote**: Quantificazione della sanzione pecuniaria in relazione alla gravità del fatto. Il valore unitario della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente. La sanzione non può essere inferiore a cento e superiore a mille quote.

m. **Reati**: Reati presupposto dell'applicazione della responsabilità delle persone giuridiche introdotta dal Decreto.

n. **Sistema Disciplinare**: Insieme delle misure sanzionatorie nei confronti dei Destinatari che non osservano il Modello Organizzativo.

o. **Soggetti Apicali**: Gli Amministratori nonché i dirigenti direttamente dipendenti dall'Organo Amministrativo.

p. **Soggetti Subordinati**: I soggetti sottoposti alla direzione dei Soggetti Apicali.

3. SCOPO DEL DOCUMENTO

Il presente documento costituisce e descrive il Modello Organizzativo per la prevenzione dei reati presupposto previsti nel Decreto.

Il presente Modello Organizzativo è elaborato tenendo in considerazione l'interazione delle procedure e delle policy, formalizzate da Infordata e dal Gruppo Digital Value, con la disciplina e le previsioni del Decreto. Tali procedure e policy completano il suddetto Modello e costituiscono parte integrante dello stesso.

L'obiettivo è invero quello di integrare il complesso delle norme di condotta, dei principi, delle *policy*, delle procedure, nonché tutti gli strumenti organizzativi ed i presidi preventivi esistenti di Infordata, al fine di garantire l'attuazione delle prescrizioni del Decreto.

4. IL DECRETO 231/2001

4.1. OGGETTO DEL DECRETO

Con il D.Lgs. n. 231/2001 (di seguito anche "Decreto 231"), emanato in data 8 giugno 2001 in esecuzione della delega di cui alla Legge 29 settembre 2000, n. 300, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", la normativa italiana in materia di responsabilità delle persone giuridiche è stata adeguata ad alcune Convenzioni Internazionali in precedenza sottoscritte dallo Stato Italiano.

Il Decreto 231 ha sancito l'introduzione della responsabilità "amministrativa" degli enti (società, consorzi, altre entità fornite e prive di personalità giuridica, associazioni) dipendente dalla commissione - o dalla tentata commissione - da parte di un soggetto a qualsiasi titolo legato all'ente, di talune fattispecie di reato (c.d. "reati-presupposto"), nell'interesse o a vantaggio dell'ente stesso.

La responsabilità prevista ai sensi del Decreto 231 non è, dunque, riconducibile allo Stato, agli enti pubblici territoriali, agli enti pubblici non economici ed a quelli che svolgono funzioni di rilievo costituzionale.

In particolare, la società è ritenuta responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da "persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso" (soggetti "in posizione apicale" o "apicali"; art. 5, comma 1, lett. a), del D.Lgs. 231/2001);

- da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (i c.d. soggetti sottoposti all'altrui direzione o vigilanza; art. 5, comma 1, lett. b), del D.Lgs. 231/2001).

In altri termini, per effetto di tale regime di responsabilità, l'ente diviene il destinatario di sanzioni, come specificate nel Decreto 231, nell'ipotesi in cui un soggetto qualificato (apicale o ad esso sottoposto) ponga in essere una determinata condotta criminosa nell'interesse o a vantaggio della persona giuridica per cui opera.

La società non risponde, invece, qualora i soggetti sopra indicati abbiano agito nell'interesse esclusivo proprio o di terzi (art. 5, comma 2, del Decreto 231).

La Relazione governativa che ha accompagnato il Decreto 231, con riferimento ai concetti di "interesse" e "vantaggio", ha chiarito che il primo ha un connotato propriamente soggettivo, collegato alla volontà dell'autore materiale del reato (l'azione, pertanto, dovrà avere come obiettivo la realizzazione di uno specifico interesse dell'ente), mentre il secondo ha una valenza di tipo oggettivo, riconducibile ai risultati effettivi della sua condotta (si tratta di fattispecie nelle quali l'autore del reato, pur non avendo agito con la diretta finalità di soddisfare un interesse dell'ente, abbia comunque realizzato un vantaggio per l'ente stesso).

La responsabilità dell'ente è autonoma rispetto a quella individuale della persona fisica autrice della violazione e la relativa sanzione applicata a carico dell'ente si aggiunge a quella comminata alla persona fisica, in conseguenza della commissione del reato.

La responsabilità prevista dal Decreto 231 è esclusa, oltre che nell'ipotesi in cui i soggetti apicali e/o i loro sottoposti abbiano agito nell'interesse esclusivo proprio o di terzi, anche se la società risulti aver adottato ed efficacemente attuato, prima della commissione dei reati, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi.

4.2. FATTISPECIE DI REATO

Le fattispecie di reato previste dal Decreto, che possono configurare la responsabilità amministrativa della Società, possono essere ricomprese nelle seguenti categorie:

- reati contro la Pubblica Amministrazione e contro il patrimonio mediante frode indebita percezione di erogazioni, truffa ai danni dello Stato di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato, o di un ente pubblico e frode nelle piccole forniture, e malversazione ai danni dello Stato, peculato e abuso d'ufficio anche quando offendono interessi finanziari dell'Unione Europea, concussione, corruzione, turbata libertà degli incanti e turbata libertà del procedimento di scelta del contraente, come indicati agli artt. 24 e 25 del Decreto;
- reati informatici (quali, ad esempi, accessi non autorizzati, violazioni di sistemi informatici o falsificazioni di documenti informatici, indicati all'art. 24 bis del Decreto);
- reati di criminalità organizzata (art. 24 ter del Decreto);
- reati di falsità in monete (quali, ad esempio, falsificazione di monete, indicati dall'art. 25 bis del Decreto);
- reati contro l'industria e il commercio (art. 25 bis 1 del Decreto);
- reati societari (quali, ad esempio, false comunicazioni sociali, falso in prospetto, illecita influenza sull'assemblea, indicati all'art. 25 ter del Decreto), nonché reati in materia di trasformazioni, fusioni e scissioni transfrontaliere;
- delitti in materia di terrorismo e di eversione dell'ordine democratico (ivi incluso l'assistenza agli associati, indicati all'art. 25 quater del Decreto);
- delitti in materia di mutilazione degli organi genitali femminili (art. 25 quater 1 del Decreto);
- reati transnazionali (quali, ad esempio, associazione a delinquere o associazione di tipo mafioso con estensione e ramificazione in più nazioni, previsti dall'art. 10 della Legge 146/2006);

- delitti contro la personalità individuale (quali, ad esempio, l'induzione alla prostituzione, la pornografia minorile, la tratta di persone e la riduzione e mantenimento in schiavitù, indicati all'art. 25 quinquies del Decreto);
- abusi di mercato: abuso di informazioni privilegiate e manipolazione del mercato (art. 25 sexies del Decreto);
- reati in materia di salute e sicurezza sul lavoro (quali l'omicidio colposo e le lesioni personali in violazione delle norme in materia di sicurezza sul lavoro, indicati dall'art 25 septies del Decreto);
- riciclaggio e violazioni similari (quali, ad esempio, riciclaggio di denaro, trasferimento fraudolento di valori o ricettazione indicati dall'art. 25 octies del Decreto);
- delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 octies.1 del Decreto);
- reati in materia di diritto d'autore (art. 25 novies del Decreto);
- reati di false dichiarazioni all'Autorità Giudiziaria (art. 25 decies del Decreto).
- reati ambientali (art. 25 undecies del Decreto);
- reati relativi al lavoro clandestino e al favoreggiamento dell'immigrazione clandestina (art. 25 duodecies del Decreto);
- reati di razzismo e xenofobia (art. 25 terdecies del Decreto);
- reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 quaterdecies del Decreto);
- reati tributari (art. 25 quinquiesdecies del Decreto);
- reato di contrabbando (art. 25 sexiesdecies del Decreto);
- delitti contro il patrimonio culturale (art. 25 septiesdecies del Decreto);
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 octiesdecies del Decreto).

- delitti contro gli animali (art. 25 undevicies del Decreto).

La Società può essere chiamata a rispondere in Italia in relazione ai reati contemplati nel Decreto, anche se commessi all'estero, nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale e purché nei suoi confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.
L'ente risponde anche degli illeciti dipendenti da delitti tentati.
In ipotesi di commissione dei delitti indicati nel Decreto 231 nella forma del tentativo, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto. Si tratta di un'ipotesi particolare di "recesso attivo", disciplinato di regola dall'art. 56, comma 4, c.p.

4.3. ADOZIONE ED ATTUAZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITA' AMMINISTRATIVA DA REATO

Come già accennato, il D.Lgs. 231/2001 attribuisce valore esimente all'adozione da parte degli enti di modelli di organizzazione, gestione e controllo finalizzati a prevenire la realizzazione dei reati di cui si rendano responsabili i soggetti apicali e i soggetti sottoposti alla direzione e vigilanza dei primi, a condizione che questi modelli siano effettivamente idonei a prevenire la commissione dei reati e che vengano adeguatamente implementati e monitorati.
In particolare, in ipotesi di reato commesso da un soggetto in posizione apicale, la società non risponde se prova che (art. 6, comma 1, del D.Lgs. 231/2001):

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione (M.O.G.) idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo della società (OdV) dotato di autonomi poteri di iniziativa e di controllo;
- i responsabili hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo indicato alla precedente lettera b).

La società avrà, dunque, l'onere di dimostrare la sua estraneità ai fatti contestati al soggetto apicale, provando la sussistenza dei sopra elencati requisiti tra loro simultanei e, di riflesso, la circostanza che la commissione del reato non deriva da una propria "colpa organizzativa", ossia dal non avere predisposto misure idonee (adeguati modelli di organizzazione, gestione e controllo) a prevenire la commissione dei reati rilevanti ai fini della responsabilità amministrativa degli enti.

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

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

In sede di accertamento processuale della responsabilità è, dunque, onere dell'accusa dimostrare l'inadeguatezza del sistema di compliance adottato dall'ente.

L'art. 7, comma 4, del Decreto 231 individua quali requisiti per un'efficace attuazione dei modelli organizzativi:

la verifica periodica e l'eventuale modifica del modello quando sono scoperte significative violazioni delle prescrizioni, ovvero quando intervengono mutamenti nell'organizzazione aziendale e/o nelle attività previste nell'oggetto sociale;

un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il Decreto 231 definisce, altresì, i requisiti essenziali che i modelli di organizzazione e di gestione devono possedere, prevedendo che:

- siano individuate le attività nel cui ambito possono essere commessi reati;
- siano stabiliti specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- siano determinate modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- siano previsti obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- sia introdotto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

4.4. SISTEMA SANZIONATORIO DEL DECRETO

Il Decreto stabilisce, nei confronti della persona giuridica, due ordini di sanzioni, pecuniarie ed interdittive, in proporzione alla natura del reato e alle dimensioni dell'azienda coinvolta.

Sanzioni Pecuniarie

Le sanzioni pecuniarie sono determinate attraverso un sistema che prevede, per ogni reato, una cornice edittale con minimo e massimo di "quote" applicabili nei confronti dell'Ente. Per rendere le sanzioni realmente efficaci, la norma attribuisce al giudice il potere di definire l'entità (tra 100 e 1.000 quote, tenuto conto dell'illecito commesso, della gravità del fatto, del grado di responsabilità dell'Ente e di quanto fatto per eliminare o attenuare le conseguenze dell'illecito e prevenirne di ulteriori) e il relativo ammontare delle "quote" con cui sanzionare l'Ente (tra euro 258,23 ed euro 1.549,37 "sulla base delle condizioni economiche e patrimoniali").

Sono previste attenuanti qualora (alternativamente) l'autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne abbia ricavato un vantaggio, ovvero ne abbia ricavato un vantaggio minimo e se il danno cagionato è di particolare tenuità.

La sanzione pecuniaria, inoltre, è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado, l'Ente ha risarcito integralmente il danno oppure ha eliminato le conseguenze dannose o pericolose del reato (ovvero si è adoperato in tal senso), ha adottato un Modello idoneo a prevenire l'ulteriore commissione del reato verificatosi e ha messo a disposizione il profitto generato dalla violazione ai fini di confisca.

Sanzioni Interdittive

Il decreto prevede, poi, sanzioni di tipo interdittivo, ovvero:

i. l'interdizione dall'esercizio delle attività;

ii. la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione del reato;

iii. il divieto di contrarre con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

iv. l'esclusione da agevolazioni, finanziamenti, contributi e sussidi nonché la revoca di quelli eventualmente già concessi;

v. il divieto di pubblicizzare beni o servizi;

vi. la confisca del prezzo o del profitto del reato;

vii. la pubblicazione della sentenza.

Ferme restando le ipotesi di riduzione delle sanzioni pecuniarie, non insorge alcuna responsabilità in capo agli Enti qualora gli stessi abbiano volontariamente impedito il compimento dell'azione ovvero la realizzazione dell'evento.

4.5. CODICI DI COMPORTAMENTO PREDISPOSTI DALLE ASSOCIAZIONI RAPPRESENTATIVE DEGLI ENTI

In ottemperanza a quanto disposto dall'art. 6 del D.Lgs. 231/2001, Confindustria ha per prima emanato un codice di comportamento per la costruzione dei modelli di organizzazione, gestione e controllo (Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001; di seguito, "Linee guida di Confindustria") fornendo, tra l'altro, le indicazioni metodologiche per l'individuazione delle aree di rischio e la struttura del modello di organizzazione, gestione e controllo[1].

In estrema sintesi, le Linee guida di Confindustria forniscono le seguenti indicazioni circa le fasi principali in cui il sistema di prevenzione dei rischi 231 dovrebbe articolarsi:

- Individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione delle fattispecie di reato rilevanti ai fini della responsabilità amministrativa degli enti.
- Predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di apposite procedure.

[1] Si vedano, da ultimo, le "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo" del giugno 2021.

Le componenti di un sistema di controllo preventivo individuate da Confindustria, con riferimento ai reati dolosi, sono:

- il codice etico (o di comportamento);
- il sistema organizzativo;
- le procedure manuali ed informatiche;
- i poteri autorizzativi e di firma;
- il sistema di controllo di gestione;
- la comunicazione al personale e sua formazione;
- con riferimento ai reati colposi:
- il codice etico (o di comportamento);
- la struttura organizzativa;
- la formazione e addestramento;
- la comunicazione e coinvolgimento;
- la gestione operativa;
- il sistema di monitoraggio della sicurezza.

Il sistema di controllo deve essere ispirato ai seguenti principi:

- ogni operazione, transazione, azione dev'essere coerente, congrua, verificabile e documentabile;
- applicazione del principio di segregazione delle funzioni (nessuno può gestire in autonomia un intero processo, ma dev'esserci una ripartizione dei compiti);
- documentazione, archiviazione e conservazione dei controlli effettuati.

- Previsione di un adeguato sistema sanzionatorio per la violazione delle norme del codice etico e delle procedure previste dal modello.
- Determinazione dei requisiti dell'organismo di vigilanza, riassumibili come segue:
  - autonomia e indipendenza;
  - professionalità;
  - continuità di azione.
- Obblighi di informazione da e verso l'Oganismo di Vigilanza ("OdV").

5. ELEMENTI DEL MODELLO DI GOVERNANCE E DELL'ASSETTO ORGANIZZATIVO GENERALE

5.1. INFORDATAS.R.L.

Infordata S.p.a. (di seguito anche "Infordata" o "Società" o "Azienda") è una società per azioni costituita in data26 aprile 1980, iscritta nel registro delle imprese il 19 febbraio 1996, con sede legale Latina (LT) Piazza Paolo VI, 1.

Infordata S.p.A. ha come unico socio Digital Value S.p.a.: la Società, pertanto, fa parte del Gruppo Digital Value.

La Società ha quale oggetto sociale A) la progettazione e lo sviluppo di programmi per automazione delle procedure aziendali, la fornitura di servizi di assistenza, consulenza, formazione e quant'altro necessario alla implementazione di sistemi informatici a favore di società ed enti, sia pubblici che privati, avvalendosi di mezzi tecnici quali elaboratori elettronici e apparecchiature similari; il commercio, il noleggio la locazione finanziaria di elaborati elettronici ed apparecchiature similari, nonché apparecchiature e programmi per l'informatica in genere, a favore di società ed enti sia pubblici che privati; la promozione di iniziative atte allo scopo di

diffondere l'impego della elaborazione elettronica dei dati. nonché ogni altra attività ritenuta necessaria, opportuna e utile al raggiungimento dell'oggetto sociale.

5.2. MODELLO DI GOVERNANCE DI INFORDATA S.P.A.

Sulla base della propria struttura organizzativa e delle attività svolte, l'Azienda ha adottato il c.d. sistema di governance tradizionale.

Il sistema di corporate governance di Infordata risulta, pertanto, attualmente così articolato:

Organo Amministrativo:

La Società è amministrata da un Consiglio di Amministrazione composto da tre membri. L'Organo Amministrativo è investito dei più ampi poteri per l'amministrazione della Società e per l'attuazione ed il raggiungimento dello scopo sociale, nei limiti di quanto consentito dalla Legge e dallo Statuto.

La rappresentanza della Società ed in giudizio spetta al Presidente del Consiglio di Amministrazione senza limitazione alcuna ed ai membri del Consiglio di Amministrazione forniti di poteri delegati, nei limiti della delega.

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

Sindaci e Organo di controllo: Il collegio sindacale è composto da 4 membri, di cui 1 supplente, e la Società ha affidato ad una Società esterna l'incarico di revisione e controllo contabile dei conti della Società.

6. IL MODELLO DI INFORDATA

6.1. OBIETTIVI PERSEGUITI DA INFORDATA CON L'ADOZIONE DEL MODELLO ORGANIZZATIVO

Infordata S.p.a. è consapevole dell'opportunità connessa all'adozione di un sistema di controllo interno ispirato ai principi di cui al D.Lgs 231/01, ai fini della prevenzione della commissione di reati da parte dei propri amministratori, dipendenti, rappresentanti, partner e fornitori.

In conformità con le sue politiche aziendali, la Società ha adottato il presente Modello Organizzativo (di seguito anche "Modello" o "MOG") e ha istituito l'Organismo di Vigilanza (di seguito anche "OdV"), con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

Il Modello, compatibilmente con la specificità del sistema di Governance della Società, si ispira ai seguenti principi di controllo e verifica:

- separazione, indipendenza ed integrazione fra le funzioni aziendali: ovvero, le varie fasi di uno stesso processo decisionale o operativo aziendale (esecuzione, controllo operativo, contabilizzazione, supervisione, autorizzazione, ecc.), per quanto possibile, non sono lasciate all'autonoma gestione di una singola persona o di una sola funzione;
- formalizzazione e coerenza dei poteri autorizzativi e di firma con le funzioni e le responsabilità aziendali;
- verificabilità e tracciabilità di ogni processo aziendale, in particolare delle transazioni e delle operazioni più significative;
- verificabilità e tracciabilità delle attività di controllo;
- continuatività del flusso delle comunicazioni per, e dall'Organismo di Vigilanza, con particolare riferimento alle informazioni concernenti le operazioni a rischio, e tempestiva informativa allo stesso Organismo di Vigilanza di anomalie o violazioni del Modello organizzativo;
- messa a disposizione dell'OdV di risorse aziendali di numero e valore ragionevole e proporzionale ai risultati attesi e ragionevolmente ottenibili;

- monitoraggio da parte dell'Organismo di Vigilanza sull'attuazione del Modello organizzativo;
- sensibilizzazione e diffusione a tutti i livelli aziendali - in base alle rispettive responsabilità - delle regole comportamentali e delle procedure istituite.

6.2. LA STRUTTURA DEL MODELLO

Il Modello della Società si compone di una Parte Generale, di una Parte Speciale e di alcuni Allegati.

La Parte Generale, costituita dal presente documento, descrive il contenuto del Decreto 231, i principi base e gli obiettivi del Modello, i compiti dell'Organismo di Vigilanza, le modalità di adozione, diffusione, aggiornamento e applicazione del MOG, le modalità di segnalazione previste dalle disposizioni sul *whistleblowing*, nonché il sistema disciplinare.

La Parte Speciale, invece, ha lo scopo di definire le regole di gestione ed i principi di comportamento che tutti i destinatari del Modello devono seguire al fine di prevenire, nell'ambito delle specifiche attività svolte in Infordata e considerate "a rischio", la commissione dei reati previsti dal D.Lgs. n. 231/2001, nonché di assicurare condizioni di trasparenza e correttezza nello svolgimento delle attività rilevanti.

6.3. DOCUMENTI AZIENDALI INTEGRATI NEL MODELLO

Devono essere considerati parti integranti e sostanziali del presente Modello di organizzazione e gestione, anche in relazione alle conseguenze in tema di applicazione delle sanzioni disciplinari conseguenti all'eventuale violazione delle disposizioni in essi contenute, i seguenti documenti aziendali:

- Statuto;
- Codice Etico della Società;
- Procedure/Policy;
- DVR.

6.4. LA METODOLOGIA SEGUITA PER LA DEFINIZIONE DEL MODELLO

Infordata ha adottato il proprio Modello in conformità ai requisiti previsti dal D.Lgs. n. 231/2001, in coerenza con il contesto normativo e regolamentare di riferimento e con le indicazioni contenute nelle Linee guida di Confindustria.

I principi e i contenuti del Modello sono destinati ai componenti degli organi sociali e amministrativi, ai dipendenti della Società ed anche a terzi soggetti chiaramente individuati (partner commerciali, consulenti, collaboratori esterni e altri soggetti aventi rapporti con la Società), con riferimento all'attività svolta nei confronti di Infordata.

L'art. 6, comma 2, lett. a), del Decreto 231 prevede espressamente che il Modello dell'ente debba "individuare le attività nel cui ambito possono essere commessi reati". L'identificazione delle attività/processi societari sensibili alla realizzazione degli illeciti ha rappresentato, pertanto, il punto di partenza dell'attività svolta per la definizione del Modello ("Attività a rischio reato" e "Processi sensibili").

È stata analizzata, quindi, la realtà operativa aziendale, con particolare riguardo alle aree in cui è risultato apprezzabile il rischio della commissione dei reati-presupposto. Parallelamente è stata condotta un'indagine sugli elementi costitutivi dei reati-presupposto allo scopo di individuare le condotte concrete che, nel contesto aziendale, potrebbero realizzare le fattispecie delittuose.

In particolare, l'iter metodologico seguito per la definizione del Modello può essere suddiviso nelle fasi di seguito descritte.

- ***Fase 1 – Raccolta ed analisi della documentazione rilevante***

L'analisi della struttura societaria ed organizzativa di Infordata ha costituito il presupposto del lavoro di redazione. A tal fine, è stata acquisita ed esaminata la seguente documentazione

Atto costitutivo e Statuto della Società;

Contratti infragruppo di servizi/consulenza esterna;

Policy, procedure operative, linee guida, disposizioni interne;

DVR.

- ***Fase 2 – Individuazione delle attività e dei processi a rischio di commissione dei reati, nonché dei presidi di controllo***

Al fine di individuare le attività a rischio di commissione dei reati-presupposto, si è proceduto alla analisi della realtà aziendale. È stato effettuato un esame della complessiva struttura aziendale volto, in particolare, all'individuazione delle modalità operative di svolgimento delle relative attività e delle competenze interne.

Preliminarmente, è stato individuato l'ambito di applicazione dei presupposti soggettivi del Decreto 231. In particolare, in relazione alle disposizioni contenute nell'art. 5, comma 1, lett. a) e b), si è proceduto ad individuare i soggetti dalla cui condotta potenzialmente illecita potrebbe derivare l'estensione della responsabilità in capo alla Società. La norma si rivolge, nella fattispecie, agli Amministratori, quali soggetti apicali, nonché ai soggetti sottoposti alla direzione e alla vigilanza di questi ultimi (dipendenti).

L'attività di analisi effettuata è stata rivolta anche a tutti coloro che a qualsiasi titolo intrattengono rapporti con la Società, i quali, in base alle proprie funzioni e responsabilità, sono coinvolti nelle attività a rischio di commissione dei reati-presupposto.

In ragione dell'attuale tipologia di *business* che caratterizza la Società ed in base alle informazioni acquisite ed all'attività svolta, si è ritenuto di concentrare la maggiore attenzione sulla valutazione della sussistenza dei profili di rischio di verificazione di alcune tipologie di reato e precisamente:

- i reati contro la Pubblica Amministrazione e contro il Patrimonio mediante frode e il reato di induzione a rendere false dichiarazioni (salvo alcune fattispecie evidenziate nella Parte A della Parte Speciale);
- i reati societari e gli abusi di mercato (salvo alcune fattispecie evidenziate nella Parte B della Parte Speciale);
- i reati di ricettazione e riciclaggio;
- i reati tributari;
- i reati in materia di salute e sicurezza sul lavoro;
- i reati in materia di somministrazione del lavoro e lavoro clandestino;
- i reati in materia di criminalità informatica (salvo alcune fattispecie evidenziate nella Parte E della Parte Speciale);
- i reati ambientali;
- i reati di criminalità organizzata;
- i reati contro l'industria e il commercio.

Nella Parte Speciale del Modello vengono indicati, relativamente a ciascuna area di rischio, i Protocolli e le procedure di cui Infordata ha deciso di dotarsi per prevenire il rischio di commissione dei singoli reati.

Di seguito si riassumono le principali attività sensibili come individuate dal *risk assessment* di Infordata:

- Riguardo ai Processi/Attività aziendali a rischio per i reati contro la Pubblica Amministrazione e il reato di induzione a rendere dichiarazioni mendaci all'Autorità giudiziaria sono considerate a titolo esemplificativo, ma non esaustivo:
  - le attività amministrative (contabilità fornitori, uscite finanziarie);
  - le attività di acquisizione di beni e servizi, tra cui la partecipazione a gare;

- i rapporti con l'Autorità Giudiziaria;
- i rapporti con la Polizia Giudiziaria;
- i rapporti con le autorità ispettive (ASL, Ispettorato del Lavoro);
- i rapporti con la Pubblica Amministrazione relativi alla partecipazione a gare;
- la selezione dei consulenti, dei professionisti esterni e degli appaltatori;
- la gestione delle risorse umane.

- Riguardo ai Processi/Attività aziendali a rischio per i reati societari e gli abusi di mercato sono considerate a titolo esemplificativo, ma non esaustivo:

  - le attività seguite per la redazione del bilancio civilistico e consolidato;
  - i rapporti con le società controllate;
  - la fatturazione (ciclo attivo e passivo);
  - la gestione di tesoreria;
  - le procedure di contabilità generale;
  - le procedure di selezione e gestione delle consulenze esterne;
  - i poteri di spesa e le autorizzazioni in tal senso;
  - la gestione delle informazioni rilevanti e delle informazioni privilegiate, le operazioni con parti correlate;
  - la gestione delle assemblee della società e dei rapporti con i soci;
  - le operazioni straordinarie sul capitale sociale.

- Riguardo ai Processi/Attività a rischio per i reati in materia di ricettazione e riciclaggio sono considerate:

  - la fatturazione (ciclo attivo e passivo);
  - le attività connesse agli acquisti di beni e servizi;
  - le attività connesse alle uscite finanziarie;

- la gestione e tenuta della contabilità aziendale per fini fiscali;
- la gestione della tesoreria;
- la gestione dei rapporti *intercompany*.

- Riguardo ai Processi/Attività a rischio per i reati tributari sono considerate:
  - la fatturazione (ciclo attivo e passivo);
  - le attività connesse agli acquisti di beni e servizi;
  - la gestione della tesoreria;
  - la gestione e tenuta della contabilità aziendale per fini fiscali;
  - le attività connesse alle uscite finanziarie;
  - la gestione dei rapporti *intercompany*.
- Riguardo ai Processi/Attività aziendali a rischio per i reati in materia di salute e sicurezza sul lavoro sono considerate:
  - le attività di monitoraggio in tema di nomina delle figure professionali previste dal d.lgs. 81/2008;
  - la formalizzazione e l'aggiornamento periodico del documento di valutazione dei rischi aziendali di cui agli artt. 17 e 28 del d.lgs. 81/2008;
  - le attività formative obbligatorie.
- Riguardo ai Processi/Attività aziendali a rischio per i reati di somministrazione del lavoro e lavoro clandestino, sono considerate:
  - le attività di selezione del personale;
  - le attività di esternalizzazione del lavoro e di appalto;
  - la selezione degli appaltatori e dei fornitori.
- Riguardo ai Processi/Attività aziendali a rischio per i reati informatici sono considerate a titolo esemplificativo, ma non esaustivo:

- le attività che regolano l'accesso ai sistemi, PC e risorse contenenti dati aziendali;
- l'utilizzo dei mezzi di comunicazione elettronica (internet, posta elettronica, etc.);
- le attività che regolano l'accesso alle reti e ai sistemi esterni.

- Riguardo ai Processi/Attività aziendali a rischio per i reati ambientali sono considerate, a titolo esemplificativo ma non esaustivo:
  - il ciclo e la gestione dei rifiuti;
  - lo smaltimento dei rifiuti speciali (ad es., toner delle stampanti).
- Riguardo ai Processi/Attività aziendali a rischio per i reati di criminalità organizzata sono considerate, a titolo esemplificativo ma non esaustivo:
  - la selezione degli appaltatori e dei fornitori;
  - l'attività di selezione e assunzione del personale:
  - l'attività di scelta del partner, RTI
- Riguardo ai Processi/Attività aziendali a rischio per i delitti contro l'industria e il commercio sono considerate a titolo esemplificativo ma non esaustivo:
  - la gestione dei rapporti con i fornitori;
  - i rapporti con gli appaltatori;
  - la gestione del magazzino;
  - la fase di commercializzazione.

- Per quanto riguarda le residue ipotesi criminose previste dal Decreto 231, si è ritenuto che la specifica attività svolta dalla Società non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa. A tale riguardo, si è pertanto ritenuto esaustivo il richiamo delle fattispecie ed il

rinvio ai principi contenuti nel Codice Etico, ove tutti i destinatari sono vincolati al rispetto di valori di tutela della personalità individuale, correttezza, moralità e rispetto delle leggi.

- ***Fase 3 – Questionari e l'analisi dei rischi***

L'elaborazione di una mappatura delle aree di rischio, anche attraverso la predisposizione di specifici questionari sottoposti alle funzioni competenti di Gruppo, ha consentito di:

- approfondire gli ambiti in cui i reati-presupposto possono essere commessi;
- verificare le attività di controllo e di monitoraggio in essere;
- approfondire il sistema delle deleghe;
- verificare l'esistenza di prassi operative seguite, ma non formalizzate all'interno di procedure;
- effettuare una prima valutazione sull'idoneità delle procedure a presidiare l'insorgere dei rischi di commissione dei reati-presupposto;
- effettuare una prima valutazione sull'idoneità dei flussi informativi e del sistema di archiviazione e tracciabilità della documentazione.

- ***Fase 4 – Definizione del Modello***

All'esito dell'attività di *risk assessment*, Infordata ha provveduto a realizzare il presente documento che costituisce il Modello di organizzazione, gestione e controllo della medesima Società, in conformità a quanto indicato all'art. 6 del Decreto 231.

Il Modello individua una serie di protocolli preventivi intesi quali insieme di regole (linee guida), principi generali e specifiche procedure di verifica e controllo, tali da poter essere ritenuti idonei a governare e prevenire i profili di rischio individuati.

Sono state, inoltre, identificate le residuali carenze di organizzazione, con la formulazione di apposite indicazioni, volte all'introduzione dei relativi principi di controllo (c.d. *gap analysis*).

È stato, altresì, predisposto un apparato sanzionatorio posto a presidio delle regole, procedure e protocolli facenti capo al Modello.

Il Modello si completa, infine, con il Codice Etico, allegato al medesimo.

6.5. PROCEDURA DI ADOZIONE DEL MODELLO

Infordata con deliberazione del Consiglio di Amministrazione ha adottato il Modello volto a prevenire la commissione dei reati-presupposto, a migliorare la governance e la vigilanza della gestione, nonché ad incentivare la cultura dell'etica e della trasparenza aziendale e si è dotata di un Codice Etico.

La Società, inoltre, ha istituito l'Organismo di Vigilanza, con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello, nonché di curarne l'aggiornamento al fine di adeguarlo ai mutamenti normativi ed aziendali.

7. IL SISTEMA INTEGRATO DEI CONTROLLI INTERNI

Il sistema dei controlli interni di Infordata è costituito dall'insieme di regole, procedure, prassi e strutture organizzative interne che mirano ad assicurare il rispetto delle strategie aziendali ed il corretto andamento dell'impresa, nonché a fornire un ragionevole affidamento circa il raggiungimento dei seguenti obiettivi:

- efficacia ed efficienza dei processi aziendali;
- attendibilità del sistema informativo finalizzato a garantire l'affidabilità e l'integrità della documentazione contabile ed economica-finanziaria diretta all'esterno;
- salvaguardia del patrimonio della Società;
- conformità dei regolamenti e procedure aziendali alla normativa vigente.

L'appartenenza di Infordata al Gruppo Digital Value comporta per la Società il recepimento dei protocolli, delle policies e delle procedure di Gruppo adottate dallo stesso.

Il sistema dei controlli interni coinvolge ogni settore dell'attività svolta dalla Società e si basa sui seguenti principi ed elementi qualificanti:

- Codice Etico;
- Sistema interno di segnalazione di condotte illecite e di violazioni del presente Modello ai sensi dell'art. 6, comma 2-bis, del D.Lgs. 231/2001 (Legge in materia di "whistleblowing");
- Definizione di protocolli;
- Poteri organizzativi e di firma assegnati in coerenza con le mansioni attribuite ed il ruolo e le responsabilità affidati;
- DVR in materia di salute e sicurezza;
- Sistema di reportistica interno e formazione del personale.

I controlli coinvolgono ogni settore dell'attività aziendale.

L'organo amministrativo ha la responsabilità gestionale dell'Azienda ed è, inoltre, responsabile di attuare il sistema dei controlli interni al fine di garantirne il corretto funzionamento.

Le operazioni svolte all'interno della Società sono supportate a livello documentale, al fine di garantire la possibilità di effettuare gli opportuni controlli da parte dell'organo amministrativo.

Tutte le risorse della Società vengono sensibilizzate sull'importanza dei controlli e sulle procedure e norme applicabili, nonché sull'importanza di un impegno attivo da parte di ciascuno, onde garantire il buon esito delle procedure di controllo.

8. IL CODICE ETICO

Il Codice Etico adottato da Infordata enuncia i principi ed i valori in base ai quali la Società svolge le sue attività e detta le norme di comportamento che tutti coloro che, direttamente o

indirettamente, stabilmente o temporaneamente, instaurino, a qualsiasi titolo, rapporti di collaborazione od operino nell'interesse della Società, devono applicare nella conduzione degli affari e nella gestione delle attività aziendali.

Il Codice Etico esplicita, altresì, i valori a cui gli Amministratori, i dipendenti e i collaboratori a vario titolo devono ispirarsi nello svolgimento dell'attività lavorativa.

Il Codice Etico, allegato al presente documento ed appositamente approvato dall'Organo Amministrativo, è da considerare, ad ogni effetto, parte integrante e sostanziale del Modello Organizzativo e, pertanto, le violazioni delle disposizioni in esso contenute sono equiparate a violazioni del Modello, con quanto ne consegue in tema di applicabilità delle sanzioni disciplinari.

9. PROTOCOLLI DI PREVENZIONE GENERALE

9.1. PRINCIPI GENERALI DI PREVENZIONE

Il sistema protocollare per la prevenzione dei reati – perfezionato dalla Società sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, dall'elaborazione giurisprudenziale, nonché dalle "*best practices*" internazionali – è stato realizzato applicando alle singole attività a rischio i seguenti Principi Generali di Prevenzione, che guidano i Protocolli Generali di cui al successivo punto 9.2. e i Protocolli Speciali.

I Principi Generali di Prevenzione sono di seguito rappresentati:

- **Regolamentazione**: esistenza di disposizioni aziendali idonee a fornire principi di comportamento, regole decisionali e modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- **Tracciabilità:**
  - ogni operazione relativa ad attività a rischio deve essere, ove possibile, adeguatamente documentata;

- il processo di decisione, autorizzazione e svolgimento dell'attività a rischio deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati con dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate;

- **Separazione dei compiti:** separazione delle fasi di proposta, di decisione/autorizzazione e di controllo, da collocarsi in capo a soggetti diversi;
- **Procure e deleghe:** i poteri autorizzativi e di firma assegnati devono essere:
  - coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese;
  - chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificandone i limiti e la natura. L'atto attributivo di funzioni deve rispettare gli specifici requisiti eventualmente richiesti dalla legge (es. delega e sub-delega in materia di salute e sicurezza dei lavoratori);
- **Attività di monitoraggio:** ha lo scopo di verificare l'aggiornamento periodico e tempestivo di procure, deleghe di funzioni nonché del sistema di controllo, in coerenza con il sistema decisionale e con l'intero impianto della struttura organizzativa. Tale attività è di competenza del Consiglio di Amministrazione sia per quanto riguarda le procure aziendali che per quanto concerne le deleghe di funzioni.

9.2. PROTOCOLLI DI PREVENZIONE GENERALE

Nell'ambito delle attività a rischio individuate per ciascuna tipologia di reato (si vedano le successive parti speciali del Modello), i Protocolli di Prevenzione Generali prevedono che:

- per tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dello Statuto e del Codice Etico;
- siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire principi di comportamento, regole decisionali e modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- per tutte le operazioni rilevanti:
  - siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché la descrizione delle relative responsabilità;
  - siano sempre documentabili e ricostruibili le fasi di formazione degli atti;
  - la Società adotti strumenti di comunicazione dei poteri di firma conferiti che ne garantiscano la conoscenza nell'ambito aziendale;
  - l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruo rispetto alle posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche;
  - non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
  - l'accesso ai dati della Società sia conforme al Regolamento 2016/679 UE e successive modifiche e integrazioni, anche regolamentari, ovvero alla normativa vigente in materia di protezione dei dati personali;
  - l'accesso e l'intervento sui dati della Società sia consentito esclusivamente alle persone autorizzate;
  - sia garantita la riservatezza nella trasmissione delle informazioni;

- i documenti riguardanti la formazione delle decisioni e l'attuazione delle stesse siano archiviati e conservati, a cura dell'area aziendale competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza. L'accesso ai documenti già archiviati è consentito solo alle persone autorizzate in base alle norme interne, nonché al Collegio Sindacale, alla Società di Revisione e all'Organismo di Vigilanza.

9.3. PROTOCOLLO RELATIVO ALL'INOSSERVANZA DELLE SANZIONI INTERDITTIVE

Nel caso in cui vengano applicate sanzioni o misure cautelari interdittive alla Società, ai sensi dell'art. 23 del Decreto, è fatto divieto a chiunque di porre in essere qualunque operazione in violazione degli obblighi e divieti di tale sanzione.

I Responsabili delle attività a rischio esercitano la necessaria supervisione al fine di identificare preliminarmente le eventuali operazioni che, ancorché solo potenzialmente, possano costituire una violazione degli obblighi e dei divieti di cui alle sanzioni o misure cautelari interdittive.

I Responsabili delle attività a rischio, nel caso in cui rilevino in una determinata operazione caratteristiche riconducibili anche in parte ad una violazione, ancorché solo potenziale, degli obblighi derivanti dalle sanzioni o dalle misure cautelari interdittive:

sospendono ogni attività inerente all'operazione in oggetto;

inviano tempestivamente specifica informativa all'Amministratore Delegato che analizza, anche per il tramite di legali esterni, l'operazione, fornendo l'interpretazione ed il dettaglio dell'iter procedurale da intraprendere.

Copia della nota informativa predisposta dal Responsabili delle aree aziendali e della documentazione predisposta dall'Amministratore Delegato è tempestivamente trasmessa all'Organismo di Vigilanza.

10. SISTEMA DELLE PROCURE E DELEGHE

10.1. I PRINCIPI GENERALI

L'organo amministrativo di Infordata è il soggetto preposto a conferire ed approvare formalmente le deleghe ed i poteri di firma, assegnati in coerenza con la struttura organizzativa interna.

Le procure e le deleghe definite all'interno della Società prevedono anche l'individuazione del livello di autonomia, nonché i poteri assegnati, i quali vengono fissati in modo coerente con il livello gerarchico del delegato/procuratore, nel rispetto dei limiti di quanto necessario all'espletamento dell'incarico oggetto della delega.

10.2. LE CARATTERISTICHE DELLE DELEGHE E PROCURE

Ogni singolo atto di delega o procura è dotato delle seguenti caratteristiche principali:

- il soggetto delegante e fonte del suo potere di delega o procura;
- il soggetto delegato, con esplicito riferimento alla funzione ad esso attribuita ed al ruolo ricoperto;
- l'oggetto, ovvero l'espressa indicazione delle attività e degli atti per i quali la delega/procura viene conferita.

Le deleghe e le procure vengono raccolte e conservate presso la sede della Società.

La specifica attribuzione di competenze e poteri consente il costante monitoraggio e, ove necessario, l'aggiornamento degli stessi, in ragione delle possibili modifiche intervenute nell'organigramma, così che risultino coerenti con la struttura aziendale e le esigenze della Società.

11. PROCEDURE AZIENDALI

La Società ha adottato protocolli e procedure per svolgere adeguatamente la propria attività, nonché per prevenire e/o risolvere problematiche connesse all'esercizio delle attività aziendali.
Ogni procedura è rivolta a determinati soggetti o categorie di soggetti, individuati in base al tipo di funzioni ovvero di mansioni che vengono affidate.
Come già evidenziato, l'operatività di Infordata si conforma a una serie di procedure adottate in sede di Gruppo Digital Value e recepite anche dalla Società stessa.
Per ogni protocollo o procedura aziendale, vengono elencate le norme o la documentazione cui fare riferimento per definirne con maggiore chiarezza il contenuto.
Infine, per ciascuna procedura viene descritta la corretta sequenza di svolgimento delle attività che devono essere realizzate per il raggiungimento dello scopo prefissato.
La Società ha recepito le seguenti procedure del Gruppo Digital Value:

a) "Processo di Gestione delle offerte tecnico commerciali";
b) "Istruzione operativa per la redazione e presentazione dell'offerta"
c) "Codice di condotta fornitori Digital Value";
d) "Politica anticorruzione Gruppo Digital Value";
e) "Politica dei diritti umani del gruppo Digital Value";
f) "Politica integrata del Gruppo Digital Value";
g) "Procedura flussi informativi organismo di vigilanza";
h) "Gestione della formazione e dello sviluppo dei dipendenti";
i) "Procedura acquisti di prodotti e servizi";
j) "Gestione dei rapporti con la PA"
k) "Gestione della conformità legislativa"
l) "Gestione della Tesoreria e dei Flussi finanziari";

m) “Procedura di coordinamento per la prevenzione del riciclaggio e della corruzione del gruppo Digital Value”;

n) “Gestione dei rischi di riciclaggio, ricettazione ed impiego di denaro o di beni di provenienza illecita”.

o) “Processo per la scelta dei partner – RTI”;

p) “Procedura Qualificazione dei Fornitori”;

q) “Procedura per la ricerca, selezione ed assunzione del personale”;

r) “Politica per la gestione delle auto aziendali”

s) “Gestione degli acquisti per l’interno”;

t) “Gestione della fiscalità”;

u) “Predisposizione del bilancio di esercizio e reporting”:

v) “Predisposizione del Bilancio Consolidato”;

“Gestione della tesoreria” Risulta inoltre recepita la Policy di “Segnalazione di condotte illecite: “*Whistleblowing*” di Gruppo.

12. ORGANISMO DI VIGILANZA

Gli artt. 6 e 7 del Decreto prevedono che l'Ente possa essere esonerato dalla responsabilità connessa alla commissione dei reati indicati nel Decreto qualora la società abbia, fra l'altro:

- adottato il modello di organizzazione, gestione e controllo e lo abbia efficacemente attuato; e
- affidato il compito di vigilare sul funzionamento e sull'osservanza del modello di organizzazione, gestione e controllo e di curarne l'aggiornamento ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo.

Il Consiglio di Amministrazione di Infordata istituisce l'Organismo di Vigilanza e ne determina la composizione in forma Collegiale.

Si precisa che il Consiglio di Amministrazione mantiene invariate tutte le attribuzioni e le responsabilità previste dalla legge, dal citato Decreto e dal codice civile in generale, alle quali si aggiunge quella relativa all'adozione, al rispetto delle disposizioni e all'efficacia del Modello Organizzativo, nonché all'istituzione dell'Organismo di Vigilanza. A tal riguardo, l'onere degli aggiornamenti e adeguamenti del Modello Organizzativo è riconducibile direttamente al Consiglio di Amministrazione di Infordata, sulla base delle considerazioni e delle proposte dell'Organismo di Vigilanza.

Al contempo, le attività necessarie e strumentali all'attuazione delle disposizioni del Modello Organizzativo sono poste in essere direttamente dalle diverse Funzioni aziendali, sotto la responsabilità del referente a capo di ciascuna Funzione.

12.1 REQUISITI DI INDIPENDENZA E AUTONOMIA DELL'ORGANISMO DI VIGILANZA

I membri dell'Organismo di Vigilanza:

- sono dotati dei requisiti di indipendenza e autonomia;
- sono dotati di onorabilità;
- posseggono un'adeguata professionalità;
- sono dotati di autonomi poteri di iniziativa e controllo;
- possiedono il requisito della continuità di azione.

12.3.1 INDIPENDENZA E AUTONOMIA

La necessaria indipendenza e autonomia dell'Organismo di Vigilanza è garantita in ragione della: collocazione in posizione gerarchica di vertice in Infordata assicurata dal riporto, in modo diretto ed esclusivo, al Consiglio di Amministrazione;

emanazione in autonomia di un proprio Regolamento, di cui è messo a conoscenza il Consiglio di Amministrazione.

12.3.2 ONORABILITÀ

I componenti dell'Organismo di Vigilanza sono individuati tra soggetti dotati dei requisiti soggettivi di onorabilità previsti dall'art. 2, D. M. 30 marzo 2000, n. 162, per i membri del Collegio Sindacale di società quotate, adottato ai sensi dell'art. 148 comma 4 del d.lgs. 58/1998 (TUF).
Costituisce in ogni caso causa di ineleggibilità o di decadenza dall'Organismo di Vigilanza:
la sentenza di condanna (o di patteggiamento), per uno dei reati presupposto previsti dal Decreto o, comunque, la sentenza di condanna (o di patteggiamento) ad una pena che comporti l'interdizione anche temporanea dagli uffici direttivi delle persone giuridiche o delle imprese;
l'irrogazione di una sanzione da parte della CONSOB, per aver commesso uno degli illeciti amministrativi in materia di abusi di mercato, di cui all'art. 187 bis ss. TUF.

12.3.3 PROFESSIONALITÀ

L'Organismo di Vigilanza può essere composto da soggetti dotati di specifiche competenze nelle attività di natura ispettiva, nell'analisi dei sistemi di controllo e in ambito giuridico, affinché sia garantita la presenza di professionalità adeguate allo svolgimento delle relative funzioni. Ove necessario, l'Organismo di Vigilanza può avvalersi anche dell'ausilio e del supporto di competenze esterne.

12.3.4 AUTONOMIA ED INDIPENDENZA

L'Organismo di Vigilanza è dotato, nell'esercizio delle sue funzioni, di autonomia ed indipendenza dagli organi societari e dagli altri organismi di controllo interno.
L'Organismo di Vigilanza dispone di autonomi poteri di spesa sulla base di un budget di spesa annuale, approvato dal Consiglio di Amministrazione su proposta dell'Organismo stesso. In ogni

caso, l'Organismo di Vigilanza può richiedere un'integrazione dei fondi assegnati, qualora non risultino sufficienti all'efficace espletamento dei propri compiti, e può estendere la propria autonomia di spesa di propria iniziativa in presenza di situazioni eccezionali o urgenti, che saranno oggetto di successiva relazione al Consiglio di Amministrazione.

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura aziendale.

L'Organismo di Vigilanza deve essere composto in maggioranza da soggetti privi di rapporti continuativi con la Società. Nell'esercizio delle loro funzioni i membri dell'Organismo di Vigilanza non devono trovarsi in situazioni, anche potenziali, di conflitto di interesse derivanti da qualsivoglia ragione di natura personale, familiare o professionale. In tale ipotesi, essi sono tenuti ad informare immediatamente gli altri membri dell'Organismo e devono astenersi dal partecipare alle relative deliberazioni.

12.3.5 CONTINUITÀ DI AZIONE

L'Organismo di Vigilanza deve essere in grado di garantire la necessaria continuità nell'esercizio delle proprie funzioni, anche attraverso la calendarizzazione dell'attività e dei controlli, la verbalizzazione delle riunioni e la disciplina dei flussi informativi provenienti dalle strutture aziendali.

12.2 NOMINA E DURATA IN CARICA DEI COMPONENTI DELL'ORGANISMO DI VIGILANZA

I componenti dell'Organismo di Vigilanza rimangono in carica per un periodo preferibilmente non superiore a tre anni e possono essere riconfermati. In caso di decadenza del Consiglio di Amministrazione che li ha nominati, per qualsiasi motivo avvenuta, i componenti dell'Organismo di Vigilanza rimarranno comunque in carica fino alla scadenza del periodo della nomina.

La nomina e la revoca dell'Organismo di Vigilanza sono di competenza del Consiglio di Amministrazione, che ha facoltà di delegare a tal fine i legali rappresentanti della Società, salvo prendere atto delle eventuali nuove nomine effettuate dai delegati.

Al riguardo, all'atto del conferimento dell'incarico, ciascun componente dell'Organismo di Vigilanza deve rilasciare una dichiarazione nella quale attesti l'assenza dei menzionati motivi di incompatibilità in relazione alla specifica attività.

È facoltà dei componenti dell'Organismo di Vigilanza rinunciare in qualsiasi momento all'incarico. In tal caso, essi devono darne comunicazione per iscritto motivando le ragioni che hanno determinato la rinuncia agli altri componenti dell'Organismo di Vigilanza e il Presidente di quest'ultimo informerà il Consiglio di Amministrazione. In caso di rinuncia da parte di uno o più membri dell'Organismo, la rinuncia non ha effetto sino all'accettazione o alla nomina del nuovo componente o dei nuovi componenti da parte del Consiglio di Amministrazione.

12.3 ATTIVITÀ E POTERI DELL'ORGANISMO DI VIGILANZA

12.3.1 ATTIVITÀ DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza ha il compito di svolgere, con autonomi poteri di iniziativa e controllo, le seguenti attività:

- vigilare sul rispetto del Codice Etico;
- verificare l'efficacia e l'adeguatezza del Modello ovvero l'idoneità a prevenire il verificarsi dei reati di cui al Decreto;
- analizzare l'attività aziendale al fine di aggiornare la mappatura delle attività a rischio;
- promuovere iniziative per la formazione dei destinatari del Modello e per la sua comunicazione e diffusione;
- raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute nel rispetto del Modello;

- vigilare affinché i comportamenti posti in essere all'interno dell'azienda corrispondano a quanto previsto dal Modello;
- qualora venga richiesto, fornire chiarimenti, delucidazioni e pareri sulla conformità di determinate situazioni e comportamenti al Modello;
- effettuare periodicamente verifiche mirate sulla base di un programma annuale;
- effettuare le altre verifiche ritenute necessarie, dandone successivamente comunicazione al Consiglio di Amministrazione;
- coordinarsi con le Funzioni aziendali al fine di acquisire informazioni utili a realizzare un costante monitoraggio dell'evoluzione delle attività a rischio;
- verificare che le azioni correttive necessarie per rendere il Modello adeguato ed efficace vengano attuate tempestivamente;
- attivare e svolgere verifiche interne per acquisire informazioni necessarie alla propria operatività;
- ricevere le segnalazioni di violazioni del Modello, svolgere tutti gli approfondimenti necessari sulla loro fondatezza e garantire la tutela della riservatezza del segnalante, ai sensi delle disposizioni in materia di "*whistleblowing*";
- segnalare i necessari aggiornamenti del Modello rispetto alle modifiche normative e alla struttura aziendale affinché il Consiglio di Amministrazione possa approvarli, mantenendo il documento coerente con le finalità descritte dal Decreto. Nell'ambito delle attività di verifica su funzionamento, efficacia e osservanza del Modello, l'Organismo di Vigilanza:
  - qualora emerga che lo stato di attuazione delle regole previste sia carente, deve adottare tutte le iniziative necessarie al fine di far adeguare i comportamenti alle previsioni del Modello;

- a fronte dell'emergere di necessità di adeguamento del Modello, deve attivarsi nel più breve tempo possibile;
- può comunicare per iscritto i risultati delle proprie verifiche ai Responsabili delle Funzioni aziendali competenti, richiedendo un piano delle azioni di miglioramento;
- deve acquisire direttamente presso le Funzioni competenti tutti gli elementi necessari per promuovere l'applicazione del sistema disciplinare.

L'Organismo di Vigilanza deve informare, nel più breve tempo possibile, il Consiglio di Amministrazione in merito ad eventuali gravi violazioni del Modello, richiedendo anche il supporto delle Funzioni aziendali in grado di collaborare nell'attività di verifica e nell'individuazione delle azioni idonee a impedire il ripetersi di tali circostanze.

Le attività poste in essere dall'Organismo di Vigilanza nell'esercizio delle proprie funzioni non potranno essere in alcun caso sindacate da alcun altro organismo o struttura aziendale, fermo restando però che il Consiglio di Amministrazione è in ogni caso tenuto a svolgere un'attività di riscontro sull'adeguatezza degli interventi dell'Organismo di Vigilanza.

12.3.2 POTERI DELL'ORGANISMO DI VIGILANZA

Per lo svolgimento dei compiti assegnatigli, all'Organismo di Vigilanza sono attribuiti i seguenti poteri e facoltà:

- accedere ad ogni tipologia di documento aziendale rilevante in relazione alle funzioni attribuitegli;
- avvalersi della collaborazione di qualsiasi funzione aziendale;
- richiedere che qualsiasi dipendente della Società fornisca tempestivamente informazioni, dati e/o notizie necessarie per individuare aspetti connessi all'attività aziendale rilevanti ai sensi del Modello e per la verifica della sua effettiva attuazione;
- richiedere al Consiglio di Amministrazione di essere convocato.

Il Consiglio di Amministrazione deve inoltre approvare annualmente, su proposta dell'Organismo di Vigilanza, un'adeguata dotazione finanziaria per lo svolgimento delle sue attività.

L'operatività dell'Organismo di Vigilanza deve essere disciplinata da un Regolamento interno, approvato dallo stesso, con particolare riferimento a composizione, compiti e strumenti, nomina, durata in carica e cause di decadenza, convocazione, voto e delibere, risorse, reporting e obbligo di informativa.

12.4 REVOCA E SOSTITUZIONE DEI COMPONENTI DELL'ORGANISMO DI VIGILANZA

Ciascun componente dell'Organismo di Vigilanza non può essere revocato se non per giusta causa, mediante apposita delibera del Consiglio di Amministrazione. A tale proposito, per giusta causa di revoca dovrà intendersi il verificarsi di una delle seguenti cause di incompatibilità:

- grave negligenza nell'assolvimento dei propri compiti;
- violazione del Modello;
- inattività ingiustificata;
- condanna, con sentenza passata in giudicato, per fatti connessi allo svolgimento dell'incarico;
- dichiarazione di interdizione, inabilitazione nonché fallimento ovvero condanna con sentenze che comportino l'interdizione dai Pubblici Uffici, dagli uffici direttivi delle imprese e delle persone giuridiche, da una professione o da un'arte, nonché l'incapacità di contrarre con la P.A.;
- sopraggiungere di una permanente condizione di conflitto di interessi;
- variazioni dell'assetto azionario che comportino il cambiamento del soggetto che dispone della maggioranza dei voti esercitabili in Assemblea Ordinaria.

Nel dettaglio, per "*grave negligenza nell'assolvimento dei propri compiti*", è da intendersi, in via esemplificativa e non esaustiva:

- l'omessa redazione delle relazioni informative sull'attività svolta al Consiglio di Amministrazione;
- l'omessa verifica delle segnalazioni di cui è destinatario, in merito alla commissione o la presunta commissione di reati di cui al Decreto, nonché alla violazione o presunta violazione del Codice Etico, del Modello o delle procedure stabilite in attuazione dello stesso;
- la mancata convocazione e tenuta di riunioni dell'Organismo di Vigilanza nel corso di un semestre;
- l'omessa verifica dell'adeguatezza dei programmi di formazione, delle modalità di attuazione e dei risultati;
- l'omessa segnalazione al Consiglio di Amministrazione degli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa che richiedono un aggiornamento del Modello;
- l'omessa segnalazione al Consiglio di Amministrazione di provvedimenti disciplinari e sanzioni eventualmente applicate dalla Società, con riferimento alle violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione nonché alle violazioni delle previsioni del Codice Etico;
- la mancata effettuazione delle attività di verifica, di routine o ad hoc, sulle attività sensibili di cui al piano delle verifiche dell'Organismo di Vigilanza.

Nel caso di "*grave negligenza nell'assolvimento dei propri compiti*", la revoca del componente dell'Organismo di Vigilanza è disposta mediante apposita delibera del Consiglio di Amministrazione, sentito il Collegio Sindacale.

13. COMUNICAZIONE, INFORMAZIONE E FORMAZIONE

13.1 REPORTING DELL'ORGANISMO DI VIGILANZA AL CONSIGLIO DI AMMINISTRAZIONE

L'Organismo di Vigilanza di Infordata riferisce formalmente in merito:

- all'attuazione del Modello Organizzativo;
- ad eventuali aspetti critici dello stesso;
- all'esito delle attività di verifica svolte nell'esercizio dei compiti assegnati.

A tal fine, l'Organismo di Vigilanza:

- formula le sue proposte al Consiglio di Amministrazione per gli eventuali aggiornamenti, modifiche ed adeguamenti del Modello Organizzativo che dovessero essere necessarie a seguito di:
  - violazioni delle prescrizioni di cui al Modello Organizzativo;
  - significative modificazioni dell'assetto interno della Società; e
  - modifiche normative;
- segnala al Consiglio di Amministrazione ogni violazione accertata del Modello Organizzativo che possa comportare l'insorgere di una responsabilità in capo alla Società per gli opportuni provvedimenti.

L'Organismo di Vigilanza predispone una relazione semestrale per il Consiglio di Amministrazione avente ad oggetto gli esiti della sua attività. L'Organismo di Vigilanza potrà predisporre altre specifiche relazioni ricorrendone la necessità.

All'Organismo di Vigilanza potrà essere richiesto di riferire in qualsiasi momento, da parte del suddetto organo, come pure l'Organismo di Vigilanza stesso potrà riferire, in merito a situazioni specifiche *e/o* ritenute pregiudizievoli.

13.2 OBBLIGHI DI INFORMAZIONE VERSO L'ORGANISMO DI VIGILANZA

Devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza, da parte dei Destinatari, sull'indirizzo di posta elettronica dedicato odv-231_infordata@digitalvalue.it, tutte le informazioni ritenute utili alla sua attività, tra cui a titolo esemplificativo:

- gli esiti degli eventuali controlli posti in essere per dare attuazione al Modello, dai quali emergano criticità;
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini inerenti alla Società, per i reati di cui al Decreto;
- comunicazioni interne ed esterne riguardanti fatti che possano essere messi in collegamento con ipotesi di reato di cui al Decreto (ad es. procedimenti disciplinari avviati/provvedimenti disciplinari adottati);
- richieste di assistenza legale inoltrate da personale nei cui confronti la Magistratura proceda per i reati previsti dal Decreto;
- richieste di chiarimenti e pareri inoltrate dal personale su tematiche attinenti la conformità al Modello di determinati comportamenti;
- esiti di verifiche interne da cui emergano responsabilità per le ipotesi di reato di cui al Decreto;
- notizie relative a cambiamenti organizzativi;
- operazioni significative o atipiche che possano essere a rischio in relazione ai reati di cui al Decreto;
- violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sui luoghi di lavoro;
- eventuali comunicazioni del Revisore riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul Bilancio della Società.

All'Organismo di Vigilanza dovrà, inoltre, essere garantito l'accesso alla documentazione elettronica e cartacea contenenti informazioni utili ai fini dell'attività del medesimo quali ad esempio l'archivio societario (verbali delle riunioni degli Organi Societari, Statuti, ecc.).

La documentazione rilevante ai fini dell'applicazione del Modello dovrà essere conservata, da parte delle Aree interessate, per un periodo di 10 anni.

L'Organismo di Vigilanza, a sua volta, è tenuto a conservare per il medesimo periodo la documentazione acquisita nell'esercizio della propria attività.

13.3 COMUNICAZIONE CON L'ORGANISMO DI VIGILANZA – POLICY WHISTLEBLOWING

Con Legge 30 novembre 2017, n. 179, in materia di "*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*", l'ordinamento italiano ha regolamentato l'istituto del c.d. "*Whistleblowing*", la cui funzione primaria è la protezione da eventuali ritorsioni verso chi, all'interno di un'organizzazione aziendale, denuncia comportamenti illeciti.

Successivamente, con l'emanazione della Direttiva (UE) 2019/1937, il diritto dell'Unione Europea ha inteso armonizzare le normative degli Stati membri sul punto. Il legislatore italiano ha recepito la Direttiva con il d.lgs. 24/2023. A seguito della promulgazione di tale corpo normativo, la Società ha adottato una policy di Gruppo, che si intende qui integralmente richiamata, che costituisce parte integrante del presente Modello e alla quale si rimanda per gli aspetti relativi ai canali di segnalazione e alla gestione di queste.

13.4 GESTIONE DELLE INFORMAZIONI DI RESPONSABILITA' DELL'ORGANISMO DI VIGILANZA

Tutte le informazioni, segnalazioni, report, etc. sono opportunamente gestiti e conservati dall'Organismo di Vigilanza in un apposito *database*.

Per l'accesso a tali dati/informazioni sono previste credenziali riservate.

Tutti i dati archiviati e custoditi dall'Organismo di Vigilanza, possono essere messi a disposizione di soggetti esterni all'Organismo di Vigilanza solo previa espressa autorizzazione scritta di quest'ultimo e della Società.

13.5 INDIVIDUAZIONE DELL'ORGANISMO DI VIGILANZA IN EUROLINKS.R.L.

In ottemperanza a quanto stabilito dall'art. 6, comma 1, lett. b), del Decreto 231 ed alla luce delle indicazioni enucleate nelle Linee guida di Confindustria, Infordata ha identificato il proprio OdV che dovrà assicurare il controllo operativo e la supervisione di tutte le regole aziendali sottoposte a vigilanza, assicurando l'efficace applicazione del Modello.

I principi generali in tema di istituzione, nomina e sostituzione dell'Organismo di Vigilanza, nonché le regole operative di funzionamento dello stesso, sono previsti nel Regolamento dell'Organismo di Vigilanza.

La nomina quale componente dell'Organismo è condizionata alla presenza ed al mantenimento dei requisiti soggettivi di eleggibilità qui indicati e poi riportati nel Regolamento dell'Organismo di Vigilanza.

Nello specifico, non devono sussistere all'atto del conferimento dell'incarico i seguenti motivi di impedimento:

- conflitti di interesse, anche potenziali, con la Società o con i soci, tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'OdV;
- rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell'OdV;
- condanna, anche non definitiva, in Italia o all'estero, per delitti rilevanti ai fini della responsabilità amministrativa degli enti o delitti ad essi assimilabili;

- condanna, anche non passata in giudicato, ovvero di patteggiamento, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei motivi di ineleggibilità dovesse configurarsi successivamente, l'OdV deve darne immediata comunicazione al C.d.A. affinché possa prendere le determinazioni necessarie.
L'Organismo potrà avvalersi, inoltre, di competenze professionali esterne alla Società, laddove l'attuazione o l'aggiornamento del MOG necessitino l'approfondimento di particolari tematiche.
Il C.d.A. di Infordata garantisce all'Organismo autonomia di iniziativa e libertà di controllo sulle attività della Società a rischio-reato, con l'obiettivo di incoraggiare il rispetto della legalità e del Modello e consentire l'immediata indagine delle violazioni.
I compensi dovuti all'OdV saranno determinati dalla Società e definiti formalmente nel contratto di assegnazione dell'incarico.

14. WHISTLEBLOWING

14.1 RIFERIMENTI NORMATIVI

Il sistema di segnalazioni denominato "*whistleblowing*" è stato introdotto in Italia con la legge n. 179 del 2017. Tale normativa regolamentava in modo completo l'istituto per la pubblica amministrazione e introduceva alcune disposizioni riferite alle organizzazioni del settore privato dotate di un modello organizzativo di gestione e controllo ex. D.Lgs. n.231/2001.
Il Decreto Legislativo n. 24/2023 - emesso in attuazione della Direttiva UE n. 2019/1937 - ha compiutamente riformato l'istituto.
La nuova normativa prevede che tutti gli enti pubblici devono dotarsi di procedure interne per la gestione delle segnalazioni; lo stesso obbligo è in carico ai soggetti del settore privato che si siano

dotati di un modello organizzativo *ex* D.Lgs. n. 231/2001 e a tutte le organizzazioni private con almeno 50 dipendenti.

14.2 I SOGGETTI CHE POSSONO EFFETTUARE UNA SEGNALAZIONE WHISTLEBLOWING

Il sistema di segnalazioni c.d. *whistleblowing* è volto a far emergere ogni utile informazione in ordine a illeciti, commessi o anche potenzialmente commessi, nell'ambito dell'operatività sociale.

Posto che lo scopo della procedura è quello di facilitare la comunicazione di informazioni relative a violazioni riscontrate durante l'attività lavorativa, la stessa si rivolge a chiunque acquisisca tali informazioni nel contesto di tale attività.

Lo spettro dei potenziali segnalanti è pertanto molto ampio.

Possono effettuare una segnalazione le seguenti categorie di soggetti:

- dipendenti;
- collaboratori;
- fornitori, subfornitori e dipendenti e collaboratori degli stessi;
- liberi professionisti, consulenti, lavoratori autonomi;
- volontari e tirocinanti, retribuiti o non retribuiti;
- azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza;
- ex dipendenti, ex collaboratori o persone che non ricoprono più una delle posizioni indicate in precedenza;
- soggetti in fase di selezione, di prova o il cui rapporto giuridico con l'ente non sia ancora iniziato;
- **clienti e soggetti terzi** (segnalazioni da parte di clienti o altre persone esterne che abbiano avuto accesso a informazioni rilevanti per l'azienda).

14.3 OGGETTO DELLA SEGNALAZIONE

Possono essere segnalati fatti illeciti di cui si sia venuti a conoscenza nel contesto della propria attività lavorativa, nonché sospetti qualificati di condotte integranti reati o altre violazioni di disposizioni di legge.

Le segnalazioni, dunque, possono riguardare illeciti penali, civili, amministrativi o contabili, così come le violazioni di normative comunitarie.

Non rientrano nell'oggetto della procedura *whistleblowing* le segnalazioni di carattere personale (per esempio inerenti al proprio contratto di lavoro).

Non viene richiesto alla persona segnalante di dimostrare in modo completo la commissione di un illecito, ma le segnalazioni devono essere quanto più possibile circostanziate, al fine di consentire un accertamento dei fatti comunicati da parte dei soggetti riceventi.

14.4 GESTORE DEL CANALE WHISTLEBLOWING

Infordata ha recepito la Policy whistleblowing del Gruppo Digital Value ed ha ritenuto di affidare all'OdV la responsabilità di gestione del canale interno *whistleblowing*.

L'OdV, pertanto, è il soggetto preposto alla ricezione e gestione delle segnalazioni di illecito. L'OdV può essere coadiuvato da soggetti terzi, a tale scopo specificamente nominati.

Il responsabile *whistleblowing* riceve le segnalazioni e dialoga con la persona segnalante per chiarire e approfondire l'oggetto della segnalazione.

Dopo una valutazione iniziale, svolge un'attività di accertamento delle informazioni segnalate, anche richiedendo specifiche informazioni ad altri uffici e funzioni interni all'organizzazione. Fornisce, inoltre, riscontri periodici alla persona segnalante e, al termine dell'attività di accertamento, comunica al segnalante l'esito delle attività di accertamento.

I possibili esiti oggetto di comunicazione alla persona segnalante sono:

- correzione di processi interni;

- avvio di un procedimento disciplinare;

trasferimento dei risultati delle attività di accertamento alla Procura della Repubblica;

archiviazione per mancanza di evidenze.

14.5 I CANALI PER LE SEGNALAZIONI

L'ente mette a disposizione delle persone segnalanti canali diversi per le segnalazioni di violazioni. In particolare, è possibile effettuare segnalazioni utilizzando l'indirizzo mail odv-231_infordata@digitalvalue.it , in uso esclusivo all'Organismo di vigilanza, ovvero attraverso il portale IS Web: https://infordata.wbisweb.it

In particolare, con riferimento a tale ultima modalità di inoltro delle segnalazioni, l'ente mette a disposizione una piattaforma informatica crittografata, che garantisce la riservatezza della persona segnalante, dei soggetti menzionati nella segnalazione e del contenuto della stessa.
La piattaforma guida la persona segnalante nel percorso di segnalazione attraverso domande aperte e chiuse, di cui alcune obbligatorie. È possibile allegare documenti alla segnalazione.
Tutte le informazioni contenute sulla piattaforma sono crittografate e possono essere lette solo dai soggetti abilitati alla ricezione della segnalazione stessa.

14.6 LE TEMPISTICHE DI GESTIONE DELLE SEGNALAZIONI

Al termine del percorso di segnalazione, la piattaforma mostra un codice di ricevuta a conferma che la segnalazione è stata consegnata e presa in carico dal soggetto ricevente.
Entro 7 giorni, il soggetto ricevente conferma alla persona segnalante la presa in carico della segnalazione e invita il soggetto segnalante a monitorare la sua segnalazione sulla piattaforma per rispondere a possibili richieste di chiarimenti o approfondimenti.

Entro 3 mesi dal giorno della presa in carico della segnalazione, il soggetto ricevente comunica alla persona segnalante un riscontro rispetto alle attività di accertamento svolte per verificare le informazioni comunicate nella segnalazione.

Il riscontro fornito entro 3 mesi può coincidere con l'esito delle attività di accertamento.

14.7 RISERVATEZZA E ANONIMATO

Il soggetto ricevente è tenuto a trattare le segnalazioni preservandone la riservatezza.

Le informazioni relative all'identità del soggetto segnalante, del soggetto segnalato e di ogni altra persona menzionata nella segnalazione sono trattate secondo i principi di confidenzialità. Allo stesso modo, sono trattate in modo confidenziale anche tutte le informazioni contenute nella segnalazione.

L'identità della persona segnalante non può essere rivelata senza il suo consenso. La conoscenza delle segnalazioni e dei relativi atti di accertamento è sottratta anche al diritto all'accesso amministrativo da parte dei soggetti interessati.

È possibile, inoltre, l'invio di segnalazioni anonime. In ogni caso, le segnalazioni vengono trattate secondo gli stessi principi di riservatezza.

L'eventuale violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dalla normativa nazionale.

Per quanto concerne, in particolare, l'ambito del procedimento disciplinare, l'identità del segnalante può essere rivelata al vertice aziendale e all'incolpato solo nei casi in cui:

- vi sia il consenso espresso del segnalante;
- la contestazione dell'addebito disciplinare risulti fondata, in tutto o in parte, sulla segnalazione e, conseguentemente, la conoscenza dell'identità del segnalante risulti indispensabile alla difesa dell'incolpato, sempre che tale circostanza venga dall'incolpato

dedotta e comprovata in sede di audizione o mediante la presentazione di documentazione difensiva.

14.8 LA GESTIONE DEI DATI PERSONALI

Le segnalazioni ricevute, le attività di accertamento e le comunicazioni tra la persona segnalante e la persona ricevente sono documentate e conservate in conformità alle prescrizioni in materia di riservatezza e protezione dei dati.

Le segnalazioni contengono dati personali e possono essere trattate e mantenute solo per il tempo necessario al loro trattamento che comprende l'analisi, le attività di accertamento e quelle di comunicazione degli esiti, oltre a una eventuale tempistica ulteriore per possibili commenti aggiuntivi. In nessun caso le segnalazioni saranno conservate oltre i 5 anni successivi alla comunicazione dell'esito delle attività di accertamento alla persona segnalante.

Nel corso delle attività di accertamento il soggetto ricevente può condividere con altre funzioni dell'ente informazioni, preventivamente anonimizzate, rispetto alle specifiche attività di competenza di queste ultime.

14.9 TUTELE E PROTEZIONI

La persona cui si fa riferimento nella segnalazione come responsabile del sospetto di illecito beneficia di misure di protezione dell'identità analoghe a quelle della persona segnalante e delle altre persone menzionate nella segnalazione.

Viene, in ogni caso, garantita protezione alla persona segnalante contro ogni forma di ritorsione o discriminazione che dovesse subire in seguito e a causa di una segnalazione.

Per ritorsione si intende qualsiasi azione o omissione minacciata o reale, diretta o indiretta, collegata o derivante da segnalazioni di illeciti effettivi o sospetti, che causi o possa causare danni fisici, psicologici, danni alla reputazione della persona, perdite economiche.

Tra le possibili discriminazioni rientrano:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- note di merito o referenze negative;
- misure disciplinari o altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o un trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto a termine;
- danni, anche alla reputazione della persona, pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

14.10 SANZIONI

Il Decreto Legislativo n. 24/2023 prevede sanzioni amministrative, irrogabili da parte dell'Autorità Nazionale Anticorruzione, in caso di violazione delle norme sul *whistleblowing*.

Le sanzioni riguardano in modo specifico eventuali ritorsioni contro i soggetti segnalanti, violazioni dell'obbligo di riservatezza, il boicottaggio a un tentativo di segnalazione, la mancata presa in carico di una segnalazione o un'insufficiente attività istruttoria avviata in seguito alla stessa.

Sono altresì sanzionabili gli abusi del sistema di segnalazione, con possibili sanzioni per colui che calunnia o diffama un altro soggetto a mezzo della procedura.

L'amministrazione può procedere disciplinarmente contro i soggetti responsabili di queste condotte.

14.11 CANALI ESTERNI PER LE SEGNALAZIONI

Al di fuori della procedura interna per le segnalazioni, la legge permette di effettuare anche segnalazioni esterne, dirette all'Autorità Nazionale Anticorruzione.

In particolare, è consentito segnalare utilizzando il canale "esterno" posto a disposizione dell'ANAC qualora sia già stata effettuata una segnalazione a cui non è stato dato seguito, qualora si abbiano fondati motivi di ritenere che ad una segnalazione interna non sia dato seguito o che questa possa determinare un rischio di ritorsione o qualora si abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le modalità di segnalazione all'Autorità Nazionale Anticorruzione sono disponibili alla pagina dedicata sul sito dell'ANAC: *anticorruzione.it/-/whistleblowing*.

In ipotesi di mancato riscontro a una segnalazione interna o esterna previamente effettuata, di pericolo imminente o palese per l'interesse pubblico, di fondati motivi che una segnalazione interna non venga trattata o che le prove della stessa possano essere distrutte o occultate è consentita, infine, la divulgazione pubblica.

15. IL SISTEMA SANZIONATORIO

15.1 PRINCIPI GENERALI

Il sistema sanzionatorio di seguito descritto è un apparato autonomo di misure finalizzato a presidiare il rispetto e l'efficace attuazione del Codice Etico e del Modello, radicando nel personale aziendale, e in chiunque collabori a qualsiasi titolo con la Società, la consapevolezza della ferma volontà di quest'ultima di perseguire qualunque violazione delle regole stabilite per il corretto svolgimento dell'attività aziendale.

L'applicazione delle sanzioni stabilite dal Modello non sostituisce né presuppone l'irrogazione di ulteriori, eventuali sanzioni di altra natura (penale, amministrativa, tributaria), che possano derivare dal medesimo fatto. Tuttavia, qualora la violazione commessa configuri anche un'ipotesi di reato oggetto di contestazione da parte dell'autorità giudiziaria, e la Società non sia in grado con gli strumenti di accertamento a sua disposizione di pervenire ad una chiara ricostruzione dei fatti, essa potrà attendere l'esito degli accertamenti giudiziali per adottare un provvedimento disciplinare.

Il rispetto delle disposizioni del Codice Etico e del Modello è applicabile ai contratti di lavoro di qualsiasi tipologia e natura, inclusi quelli con i dirigenti, a progetto, part-time, ecc., nonché nei contratti di collaborazione rientranti nella c.d. para subordinazione.

Il procedimento disciplinare viene avviato su impulso dell'Organismo di Vigilanza che svolge, altresì, una funzione consultiva nel corso del suo intero svolgimento.

In particolare, l'Organismo di Vigilanza, acquisita la notizia di una violazione o di una presunta violazione del Codice Etico o del Modello, si attiva immediatamente per dar corso ai necessari accertamenti, garantendo la riservatezza del soggetto nei cui confronti si procede.

Se viene accertata la violazione da parte di un dipendente della Società (intendendo ogni soggetto legato alla Società da un rapporto di lavoro subordinato), l'Organismo di Vigilanza informa immediatamente il titolare del potere disciplinare.

Qualora si verifichi una violazione da parte dei collaboratori o dei soggetti esterni che operano su mandato della Società, l'Organismo di Vigilanza informa con relazione scritta il Presidente e l'Amministratore Delegato.

Il titolare del potere disciplinare avvia i procedimenti di sua competenza con riferimento alle contestazioni e all'eventuale applicazione delle sanzioni.

Le sanzioni per le violazioni delle disposizioni del Codice Etico e del presente Modello sono adottate dal titolare del potere disciplinare.

15.2 VIOLAZIONI DEL MODELLO E DEL CODICE ETICO

Costituiscono infrazioni tutte le violazioni, realizzate anche con condotte omissive e in eventuale concorso con altri, delle prescrizioni del presente Modello, dei Protocolli di Prevenzione, delle relative procedure di attuazione, delle specifiche procedure integrate al Modello nonché delle violazioni delle previsioni del Codice Etico.

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni comportamenti che costituiscono infrazione:

- la redazione, in modo incompleto o non veritiero, di documentazione prevista dal presente Modello, dai Protocolli di Prevenzione e dalle relative procedure complementari;
- l'agevolazione della redazione, da altri effettuata in modo incompleto e non veritiero, di documentazione prevista dal presente Modello, dai Protocolli di Prevenzione e dalle relative procedure complementari;
- l'omessa redazione della documentazione prevista dal presente Modello, dai Protocolli e dalle procedure di attuazione;

- la violazione o l'elusione del sistema di controllo previsto dal Modello, in qualsiasi modo effettuata, (ad esempio, attraverso la sottrazione, la distruzione o l'alterazione della documentazione inerente la procedura, l'ostacolo ai controlli, l'impedimento all'accesso alle informazioni e alla documentazione nei confronti dei soggetti preposti ai controlli delle procedure e delle decisioni);
- l'omessa comunicazione all'Organismo di Vigilanza delle informazioni prescritte;
- la violazione o l'elusione degli obblighi di vigilanza da parte dei Soggetti Apicali nei confronti dell'operato dei propri subordinati;
- la violazione degli obblighi in materia di partecipazione ai programmi di formazione;
- l'adozione di atti di ritorsione, discriminazione o penalizzazione, diretti o indiretti, nei confronti di chi abbia segnalato condotte illecite all'Organismo di Vigilanza;
- la falsa segnalazione di condotte illecite, commessa con dolo o colpa grave.

15.3 SANZIONI E MISURE DISCIPLINARI

Il Codice Etico e il Modello costituiscono un complesso di norme alle quali il personale dipendente di una società deve uniformarsi anche ai sensi di quanto previsto dagli artt. 2104 e 2106 c.c. e dai Contratti Collettivi Nazionali di Lavoro (CCNL) in materia di norme comportamentali e di sanzioni disciplinari. Pertanto, tutti i comportamenti tenuti dai dipendenti in violazione delle previsioni del Codice Etico, del Modello e delle sue procedure di attuazione, costituiscono inadempimento alle obbligazioni primarie del rapporto di lavoro e, conseguentemente, infrazioni, comportanti la possibilità dell'instaurazione di un procedimento disciplinare e la conseguente applicazione delle relative sanzioni.

15.3.1 Sanzioni nei confronti dei dipendenti

Nei confronti dei lavoratori dipendenti con qualifica di operaio, impiegato e quadro sono, nel caso di specie, applicabili – nel rispetto delle procedure previste dall'art. 7 della legge 20 maggio 1970

n. 300 (Statuto dei Lavoratori) – i provvedimenti previsti dai CCNL terziario e CCNL industria/metalmeccanico.

Nel rispetto dei principi di gradualità e proporzionalità, il tipo e l'entità delle sanzioni irrogabili saranno determinati in base ai seguenti criteri:

- gravità delle violazioni commesse;
- mansioni e posizione funzionale delle persone coinvolte nei fatti;
- volontarietà della condotta o grado di negligenza, imprudenza o imperizia;
- comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari, nei limiti consentiti dalla legge e dal CCNL;
- altre particolari circostanze che accompagnano la violazione disciplinare.

Sulla base dei principi e criteri sopra indicati:

- i provvedimenti di *richiamo verbale*, di *ammonizione scritta,* di *multa* e *di sospensione dal lavoro e dalla retribuzione* troveranno applicazione qualora il dipendente violi le procedure previste dal Modello o comunque tenga, nell'espletamento di attività nelle aree a rischio di commissione di reati, un comportamento non conforme alle prescrizioni del Modello stesso o del Codice Etico, ricorrendo l'ipotesi di cui all'art. 2104 c.c. In particolare, troverà normalmente applicazione il provvedimento della *multa non superiore all'importo di tre ore di retribuzione oraria*. In caso di maggiore gravità o di recidiva nelle mancanze di cui sopra tale da non concretizzare gli estremi del licenziamento, si potrà procedere all'applicazione della sospensione dal lavoro e dalla retribuzione fino a tre giorni, mentre nei casi di minore gravità si può procedere al rimprovero verbale o scritto;
- il provvedimento di *licenziamento con preavviso* (per giustificato motivo) troverà applicazione allorché il lavoratore adotti, nell'espletamento di attività nelle aree a rischio di commissione di reati, un comportamento non conforme alle prescrizioni del presente Modello o del Codice

Etico, tale da configurare un notevole inadempimento degli obblighi contrattuali o una condotta gravemente pregiudizievole per l'attività di Infordata, l'organizzazione del lavoro e il regolare funzionamento di essa come ad esempio:

- qualsiasi comportamento diretto in modo univoco al compimento di un reato previsto dal Decreto;
- qualsiasi comportamento volto a dissimulare la commissione di un reato previsto dal Decreto;
- qualsiasi comportamento che contravvenga deliberatamente alle specifiche misure previste dal Modello e dalle relative procedure attuative, a presidio della sicurezza e salute dei lavoratori;

- il provvedimento di *licenziamento senza preavviso* (per giusta causa) sarà applicato in presenza di una condotta consistente nella grave e/o reiterata violazione delle norme di comportamento e delle Procedure contenute nel Modello ovvero delle prescrizioni del Codice Etico, in quanto comportamento tale da non consentire la prosecuzione nemmeno provvisoria del rapporto di lavoro.

15.3.2 Sanzioni nei confronti dei dirigenti

Il rapporto dirigenziale si caratterizza per la natura eminentemente fiduciaria. Il comportamento del dirigente oltre a riflettersi all'interno della Società, costituendo modello ed esempio per tutti coloro che vi operano, si ripercuote anche sull'immagine esterna della medesima. Pertanto, il rispetto da parte dei dirigenti della Società delle prescrizioni del Codice Etico, del Modello e delle relative procedure di attuazione costituisce elemento essenziale del rapporto di lavoro dirigenziale.

Se la violazione riguarda un dirigente della Società, l'Organismo di Vigilanza deve darne comunicazione, oltre che al titolare del potere disciplinare, anche al Consiglio di

Amministrazione, in persona del Presidente e dell'Amministratore Delegato, mediante relazione scritta.

Nei confronti dei dirigenti che abbiano commesso una violazione del Codice Etico, del Modello o delle procedure stabilite in attuazione del medesimo, la funzione titolare del potere disciplinare avvia i procedimenti di competenza per effettuare le relative contestazioni e applicare le misure sanzionatorie più idonee, in conformità con quanto previsto dal CCNL Dirigenti e, ove necessario, con l'osservanza delle procedure di cui all'art. 7 della Legge 30 maggio 1970, n. 300.

Le sanzioni devono essere applicate nel rispetto dei principi di gradualità e proporzionalità rispetto alla gravità del fatto e della colpa o dell'eventuale dolo. Tra l'altro, con la contestazione può essere disposta cautelativamente la revoca delle eventuali procure affidate al soggetto interessato, fino alla eventuale risoluzione del rapporto in presenza di violazioni così gravi da far venir meno il rapporto fiduciario con la Società.

15.3.3 Sanzioni nei confronti degli Amministratori

Infordata valuta con estremo rigore ogni violazione del presente Modello realizzata da coloro che rivestono i ruoli di vertice in seno alla Società, e che, per tale ragione, sono più in grado di orientare l'etica aziendale e l'operato di chi opera nella Società ai valori di correttezza, legalità e trasparenza.

Se la violazione riguarda un Amministratore della Società, l'Organismo di Vigilanza deve darne immediata comunicazione al Revisore e al Consiglio di Amministrazione, in persona del Presidente e dell'Amministratore Delegato, se non direttamente coinvolti, mediante relazione scritta.

Nei confronti degli Amministratori che abbiano commesso una violazione del Codice Etico, del Modello o delle procedure stabilite in attuazione del medesimo, il Consiglio di Amministrazione può applicare, nel rispetto dei principi di gradualità e proporzionalità rispetto alla gravità del fatto

e della colpa o dell'eventuale dolo, ogni idoneo provvedimento consentito dalla legge, fra cui le seguenti sanzioni:

- richiamo formale scritto;
- sanzione pecuniaria pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;
- revoca, totale o parziale, delle eventuali deleghe.

Nei casi più gravi, e comunque, quando la mancanza sia tale da ledere la fiducia della Società nei confronti del responsabile, il Consiglio di Amministrazione convoca l'Assemblea dei Soci, proponendo la revoca dalla carica.

15.3.4 Sanzioni nei confronti del Sindaco/Revisore Unico

Qualora a commettere la violazione sia il sindaco/Revisore Unico, l'Organismo di Vigilanza deve darne immediata comunicazione al Consiglio di Amministrazione, in persona del Presidente e dell'Amministratore Delegato.

I soggetti destinatari dell'informativa dell'Organismo di Vigilanza potranno assumere, secondo quanto previsto dallo Statuto, gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'Assemblea dei Soci, al fine di adottare le misure più idonee previste dalla legge.

Il Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, propone all'Assemblea dei Soci l'adozione dei provvedimenti di competenza e provvede agli ulteriori incombenti previsti dalla legge.

15.3.5 Sanzioni nei confronti di collaboratori e soggetti esterni operanti su mandato della Società

Per quanto concerne i collaboratori o i soggetti esterni che operano su mandato della Società, l'Amministratore Delegato determina le misure sanzionatorie e le modalità di applicazione per le violazioni del Codice Etico, del Modello e delle relative procedure integrate. Tali misure potranno

prevedere, per le violazioni di maggiore gravità, e comunque quando le stesse siano tali da ledere la fiducia della Società nei confronti del soggetto responsabile delle violazioni, la risoluzione del rapporto e, se del caso, il risarcimento dei danni derivati a Infordata da tali violazioni.

Qualora si verifichi una violazione da parte di questi soggetti, l'Organismo di Vigilanza informa, con relazione scritta, il Presidente e l'Amministratore Delegato.

In sede di sottoscrizione degli incarichi o dei contratti è dato avviso dell'obbligo di rispetto delle previsioni del Codice Etico, del Modello e delle procedure integrate, nonché delle relative sanzioni. Tali disposizioni vengono esplicitamente sottoscritte per accettazione dai soggetti esterni.

16. COMUNICAZIONE E FORMAZIONE

La Società garantisce nei confronti di tutti i dipendenti e di tutti i soggetti con funzione di gestione, amministrazione, direzione e controllo una corretta conoscenza e divulgazione del Modello e del Codice Etico.

Il Modello ed il Codice Etico sono comunicati a tutto il personale della Società e a tutti i membri degli organi sociali, attraverso i mezzi ritenuti più opportuni.

Copia della Parte Generale del Modello e del Codice Etico è, altresì, pubblicata sul sito internet della Società.

Per i soggetti esterni alla Società destinatari del Modello e del Codice Etico sono previste apposite forme di comunicazione del Modello e del Codice Etico. I contratti che regolano i rapporti con tali soggetti devono prevedere chiare responsabilità in merito al rispetto delle politiche di impresa della Società e in particolare del suo Codice Etico e l'accettazione dei principi generali del Modello.

La Società si impegna ad attuare programmi di formazione con lo scopo di garantire l'effettiva conoscenza del Codice Etico e del Modello da parte dei dipendenti e dei membri degli organi sociali.

I programmi di formazione hanno ad oggetto il Decreto e il quadro normativo di riferimento, il Codice Etico e il presente Modello. La formazione è modulata in relazione alla qualifica dei destinatari e al diverso livello di coinvolgimento degli stessi nelle attività sensibili.

Le iniziative di formazione possono svolgersi anche a distanza mediante l'utilizzo di sistemi informatici (es.: video conferenza*, e-learning*).

La formazione del personale ai fini dell'attuazione del Modello è coordinata dall'Amministratore Delegato. L'Organismo di Vigilanza verifica l'adeguatezza dei programmi di formazione e le modalità di attuazione.

La partecipazione ai programmi di formazione di cui al presente punto ha carattere di obbligatorietà. La violazione di tali obblighi costituendo violazione del Modello risulta assoggettata alle previsioni del sistema sanzionatorio.

16.1 FORMAZIONE DEL PERSONALE IMPIEGATO NELLE AREE DI RISCHIO

La formazione del personale dirigente, del personale munito di poteri di rappresentanza e del personale non dirigente impiegato nelle attività a rischio di Infordata deve essere adeguata e provvista di periodici aggiornamenti e specifiche comunicazioni agli interessati.

L'Organismo di Vigilanza provvederà a definire programmi di formazione mirati ogni qualvolta vengano individuate esigenze specifiche e/o modifiche significative al Modello.

16.2 FORMAZIONE DEL PERSONALE NEO ASSUNTO

Con riguardo al personale neoassunto è prevista un'attività informativa e di formazione basata su:

- la consegna, unitamente alla lettera di assunzione, di una copia del Codice Etico e di una comunicazione informativa sul Modello di Organizzazione e Gestione adottato dalla Società;
- la partecipazione ad eventi formativi da cui sia possibile acquisire le conoscenze considerate di primaria rilevanza in materia di Decreto Legislativo 231/01.

Successivamente alla formazione e informazione iniziale possono seguire ulteriori iniziative formative in relazione all'incarico che il personale neoassunto va a ricoprire.

16.3 FORMAZIONE DI ALTRO PERSONALE

La formazione del personale non rientrante nelle categorie di cui ai precedenti paragrafi avviene mediante la periodica pubblicazione di documentazione informativa a cura dell'Organismo di Vigilanza.

16.4 INFORMATIVA A TERZI

I soggetti terzi (fornitori, consulenti e terzi in genere) vengono informati sulle regole di comportamento adottate dalla Società mediante idonea diffusione sul portale internet di Infordata sia del Codice Etico, sia del Modello Organizzativo.
Inoltre, è richiesto che i soggetti terzi che collaborano con la Società rilascino una dichiarazione sottoscritta (anche sotto forma di specifica clausola contrattuale) ove attestino la conoscenza del contenuto del Codice Etico e del Modello e l'impegno a osservarne le prescrizioni, nonché a non tenere condotte che possano comportare il coinvolgimento della Società in reati di cui al Decreto.

17. ADOZIONE DEL MODELLO – CRITERI DI AGGIORNAMENTO E ADEGUAMENTO DEL MOG

17.1 VERIFICHE E CONTROLLI DEL MOG

L'Organismo di Vigilanza redige il c.d. Piano delle attività attraverso il quale indica le attività di vigilanza previste nel periodo considerato, fornisce un calendario delle stesse, determina le cadenze temporali dei controlli e prevede la possibilità di effettuare verifiche e controlli non programmati.

Nello svolgimento di tali attività, l'OdV si avvale delle strutture interne alla Società con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo, nonché di consulenti esterni, ove necessario.

Nel caso in cui la Società decida di avvalersi di consulenti esterni, questi dovranno sempre riferire i risultati del loro operato all'OdV.

All'Organismo sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli.

17.2 AGGIORNAMENTO E ADEGUAMENTO

Il C.d.A. decide in merito all'aggiornamento del Modello 231 ed al suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- violazioni accertate delle prescrizioni del MOG;
- revisione periodica dello stesso, anche in relazione a modificazioni dell'assetto organizzativo della Società e/o delle modalità di svolgimento delle attività d'impresa;
- novità legislative, con riferimento alla disciplina della responsabilità amministrativa degli enti per gli illeciti amministrativi dipendenti da reato;
- risultati delle verifiche svolte dall'OdV.

Una volta approvate, le modifiche e le istruzioni per la loro immediata applicazione sono comunicate all'Organismo di Vigilanza il quale, a sua volta, provvede, senza indugio, a curare la

corretta comunicazione delle modifiche all'interno e all'esterno della Società, nonché a verificare che le predette modifiche siano attuate.

L'OdV conserva, in ogni caso, precisi compiti e poteri in merito alla cura, sviluppo e promozione del costante aggiornamento del MOG. A tal fine, può formulare osservazioni e proposte, attinenti all'organizzazione ed il sistema di controllo, alle strutture aziendali a ciò preposte o, in casi di particolare rilevanza, direttamente al C.d.A.

Nello specifico, al fine di garantire che le variazioni del MOG siano effettuate con la necessaria tempestività ed efficacia, il C.d.A. ha ritenuto di delegare all'Organismo il compito di apportare con cadenza periodica, ove risulti necessario, le modifiche al Modello 231 che attengano ad aspetti di carattere meramente descrittivo[2].

Rimane, in ogni caso, di esclusiva competenza della Società la delibera di aggiornamenti e/o di adeguamenti del MOG dovuti ai seguenti fattori:

- intervento di modifiche normative significative in tema di responsabilità amministrativa degli enti;
- identificazione di nuove attività sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività d'impresa, per il tramite di specifico *risk assessment*;
- commissione dei reati (e degli illeciti amministrativi) rilevanti ai fini della responsabilità amministrativa degli enti da parte dei soggetti destinatari del Modello 231 o, più in generale, di significative violazioni del Modello 231 stesso;
- riscontro di carenze e/o lacune nelle previsioni del MOG, a seguito di verifiche sull'efficacia del medesimo.

[2] Si precisa che con l'espressione "aspetti descrittivi" si fa riferimento ad elementi ed informazioni che derivano da atti decisi dal C.d.A. (come, ad esempio la ridefinizione dell'organigramma) o da funzioni aziendali munite di specifica delega (es. nuove procedure aziendali).