

# Modello di Organizzazione e di Gestione

*Decreto legislativo dell'8 giugno 2001, n.231 recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"*

## Infodata S.p.A.

### Parte Generale

*Adottato dal Consiglio di Amministrazione di Infodata S.p.A. con approvazione nella seduta del 24 giugno 2021*

Versione	Data	Descrizione documento, della modifica o revisione	CdA	Controllo OdV	Controllo DG
1.0	24/06/2021	Prima emissione e adozione	//	//	//
2.0	30/05/2022	1) Recepimento UNI ISO 45001:2018 2) Aggiornamento normativo art.25-octies.1	//	//	//
3.0	14/12/2023	Adeguamento al d.lgs.24/2023	//	//	//

*Questo documento è di proprietà della Infodata S.p.A. Ogni divulgazione e riproduzione o cessione di contenuti a terzi deve essere preventivamente ed espressamente autorizzata in forma scritta dalla stessa Società.*

## Sommario

1.	Presentazione della società .....	3
2.	Oggetto sociale.....	3
3.	Governance e assetto organizzativo.....	4
3.1	Il sistema di gestione per la salute e sicurezza sul lavoro (SGSL).....	7
4.	La disciplina del decreto legislativo n.231 del 2001.....	7
4.1	Principi generali.....	7
4.2	Il contenuto del Decreto .....	8
4.3	Il presupposto della punibilità dell'ente.....	9
4.4	La condizione esimente della responsabilità amministrativa dell'ente.....	10
4.4.1	Primo profilo soggettivo: reato commesso da un soggetto posto in posizione apicale .....	10
4.4.2	Il contenuto del Modello organizzativo di gestione e controllo a fini esimenti. ....	11
4.4.3	Il sistema di gestione delle segnalazioni di illecito di Infodata S.p.A. ....	12
4.5	Secondo profilo soggettivo: reato commesso da soggetti "sottoposti". ....	14
4.6	L'apparato sanzionatorio .....	15
5.	Il fenomeno del Gruppo di società e l'applicazione del d.lgs.231/01.....	18
5.1	Responsabilità della controllata per i reati commessi da soggetti appartenenti alla capogruppo .....	20
5.2	Responsabilità della controllante per i reati commessi da soggetti appartenenti alla organizzazione della controllata.....	20
5.3	I modelli organizzativi nell'ambito dei gruppi.....	22
6.	Organismo di Vigilanza.....	22
6.1	I requisiti.....	22
6.2	Composizione e individuazione.....	23
6.3	Nomina dell'OdV Infodata S.p.A.....	23
6.4	Funzioni e poteri dell'Organismo di Vigilanza .....	24
6.5	Durata in carica, decadenza e revoca .....	25
6.6	Flussi informativi dell'ODV nei confronti del vertice societario.....	25
6.7	Budget 26	
7.	Il progetto di adeguamento alla normativa intrapreso da Infodata S.p.A.....	26
7.1	Obiettivi e finalità perseguiti con l'adozione del Modello 231 .....	26
7.2	Elementi fondamentali del Modello.....	27
7.3	Modello, Codice Etico e Sistema disciplinare .....	28
7.4	Il ruolo delle Linee guida di Confindustria e l'applicazione delle norme nella costruzione del Modello.....	29
7.5	La costruzione del MOG di Infodata S.p.A.: il "Progetto 231" .....	30
8.	Destinatari del Modello .....	31
9.	Il sistema sanzionatorio 231 di Infodata S.p.A.....	31
9.1	Violazione del Modello.....	32
9.2	Misure nei confronti dell'Organo Amministrativo .....	32
9.3	Misure nei confronti dei Sindaci, Revisori e ODV .....	33
9.4	Misure e sanzioni nei confronti dei dipendenti.....	33
9.5	Le misure e le sanzioni nei confronti dei soggetti aventi rapporti contrattuali con la società.....	33
10.	Modifica, implementazione e verifica del funzionamento del Modello.....	33
10.1	Modifiche ed integrazioni dei principi di riferimento del Modello .....	33
10.2	Implementazione del Modello ed attuazione dei controlli sulle aree di attività a rischio .....	33
11.	Informazione, formazione ed aggiornamento.....	34

## 1. Presentazione della società

Infodata S.p.A. (d'ora in avanti, anche, la "Società") opera dal 1981, prima come società in nome collettivo, poi come società a responsabilità limitata e poi come società per azioni, nel mercato dell'*Information and Communication Technology*, supportando le più importanti e diffuse piattaforme hardware e software, sulle quali ha sviluppato la capacità di erogare servizi a valore aggiunto nel campo della progettazione, sviluppo e fornitura di soluzioni infrastrutturali ed applicative.

Nell'arco di 40 anni, Infodata si è modellata alle mutate esigenze di business, ha ampliato la sua struttura con una serie di acquisizioni, dove operano aziende e divisioni con competenze specifiche nelle varie aree di business.

Nata con la vocazione ad operare nel mercato delle PMI, Infodata ha progressivamente esteso il suo raggio di azione a clienti di fascia più alta come banche e finanza e pubblica amministrazione centrale e locale.

La sede legale della Società è fissata in Latina (LT) ha deciso di dotarsi di un sistema di amministrazione e controllo tradizionale basato su:

<b>CONSIGLIO DI AMMINISTRAZIONE</b> ■ 3 componenti Presidente CDA Consigliere/Amministratore Delegato Consigliere	<b>COLLEGIO SINDACALE</b> ■ 3 componenti effettivi ■ 2 componenti supplenti	<b>REVISORE LEGALE</b>
---	---	------------------------

Al fine di raggiungere l'oggetto sociale, così come risultante dallo Statuto, il Consiglio di Amministrazione nella seduta del 18 luglio 2019, ha delineato nello specifico i poteri, confermando procure speciali ed assegnato nomine ai singoli amministratori, così come risultante dall'allegato A - *Poteri di carattere gestionale nell'ambito dell'ordinaria amministrazione* - nonché dall'allegato B - *Poteri in materia di sicurezza (generali)* - nonché dall'allegato C - *Poteri in materia di Delega Privacy*.

## 2. Oggetto sociale

La *mission* di Infodata S.p.A. è dare supporto al cliente nel governare la complessità delle nuove architetture informatiche, controllando la dinamica dell'innovazione tecnologica, razionalizzando le metodologie di analisi, progettazione, realizzazione e test del software, erogando servizi di gestione delle infrastrutture e servizi di valutazione della sicurezza informatica. Tale ampiezza di contenuti ha portato la Società a dotarsi di tre sedi operative in Roma.

Rinviano allo Statuto per maggiori dettagli sull'oggetto sociale prefissato dalla Società, qui succintamente sono elencate le principali attività, realizzabili tanto in territori nazionale, quanto all'estero, anche mediante la partecipazione a gare d'appalto o licitazioni private indette dalla pubblica amministrazione o privati:

- progettazione e sviluppo di programmi per l'automazione delle procedure aziendali, la fornitura di servizi di assistenza, consulenza, formazione e quant'altro necessario per l'implementazione di

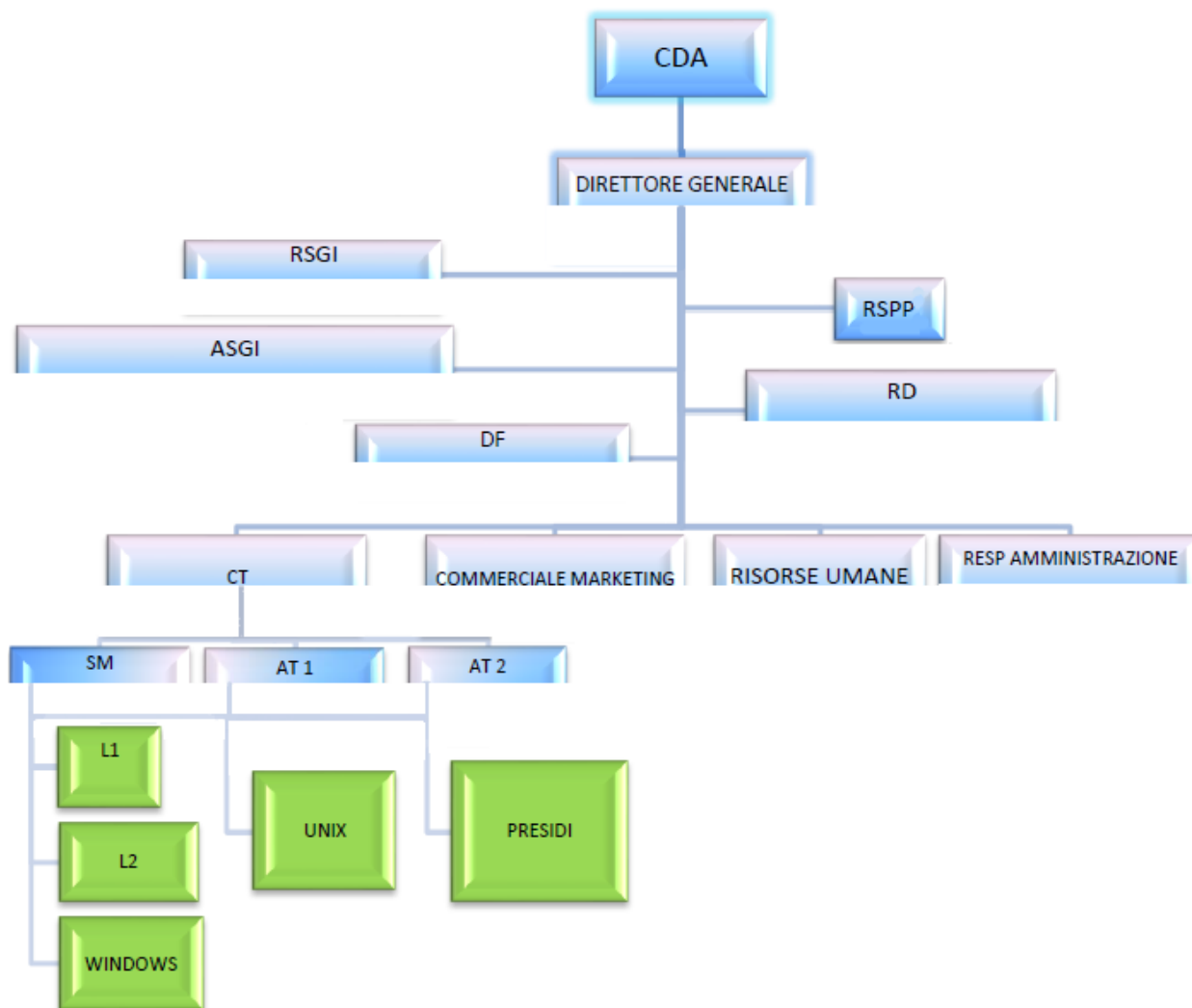
sistemi informatici a favore di società ed enti, sia pubblici che privati;

- commercio, noleggio, locazione finanziaria di elaboratori elettronici ed apparecchiature similari, nonché apparecchiature e programmi per l'informatica in genere, a favore di società ed enti pubblici o privati.

### 3. Governance e assetto organizzativo

Nel rispetto dei principi normativi in tema di gestione societaria delle società di capitali, Infordata S.p.A. ha inteso delineare il proprio assetto organizzativo interno distribuendo su vari organi e funzioni, porzioni di business che, opportunamente governate anche a livello gestionale attraverso la definizione di un Sistema di Gestione Integrato o "SGI" e l'adesione a sistemi di certificazione rilasciati da enti riconosciuti a livello internazionale, contribuiscono al raggiungimento dello scopo sociale. Questo Sistema racchiude un Sistema di Gestione Qualità o "SGQ", un Sistema di Gestione per la Sicurezza delle Informazioni, o "SGSI", un Sistema di Gestione Ambientale, o "SGA" e un Sistema di Gestione del Servizio, o "SGS".

L'organizzazione interna, pertanto, è suddivisa secondo il seguente schema:



Acronimi del SGI:

<b>FUNZIONE</b>	<b>SIGLA</b>
<b>Direttore Generale</b>	<b>DG</b>
<b>Responsabile Sistema di Gestione Integrato</b>	<b>RSGI</b>
<b>Assistente al Sistema di Gestione Integrato</b>	<b>ASGI</b>
<b>Risorse Umane</b>	<b>RU</b>
<b>Commerciale &amp; Marketing</b>	<b>DC</b>
<b>Direttore Finanza</b>	<b>DF</b>
<b>Rappresentante dell'Alta Direzione</b>	<b>RD</b>
<b>Responsabile del Servizio di Prevenzione e Protezione</b>	<b>RSPP</b>
<b>Coordinatore Tecnico</b>	<b>CT</b>
<b>Responsabile Amministrazione</b>	<b>RA</b>
<b>Service Manager</b>	<b>SM</b>
<b>Area Tecnica 1</b>	<b>AT 1</b>
<b>Area Tecnica 2</b>	<b>AT 2</b>

Al fine di rendere un servizio sempre in linea con i dettami normativi, nonché le aspettative della clientela, la Società ha deciso di adottare il Sistema di Gestione che potesse da un lato, offrire un valido sostegno tecnico-organizzativo a chi opera all'interno della Società per esser sempre *compliant* con quanto richiesto dalle norme tecniche di riferimento e, dall'altro, un apparato procedurale capace di definire i ruoli e le singole responsabilità nell'operatività quotidiana. Il SGI, quindi, rappresenta uno dei presidi posti in essere dalla Società al fine di segmentare le funzioni e responsabilizzare le risorse, in linea con le politiche di legalità impresse anche attraverso l'adozione del Codice Etico e di Comportamento.

<b>PROCESSI</b>	<b>STRUTTURE RESPONSABILI</b>
<b>Gestione e controllo sullo stato della sicurezza</b>	<b>Direzione Generale</b>
<b>Sistemi di gestione (SGQ - SGSI - SGA - SGS)</b>	<b>Direzione Generale / RSGI</b>
<b>Service desk, application management, assistenza sistemistica</b>	<b>Service desk, application management, assistenza sistemistica</b>
<b>Servizi IT</b>	<b>Servizi IT</b>
<b>Acquisti</b>	<b>Acquisti</b>
<b>Area Contabile</b>	<b>Area Contabile</b>
<b>Personale</b>	<b>Personale</b>
<b>Area Risorse Umane</b>	<b>Area Risorse Umane</b>
<b>Clienti</b>	<b>Clienti</b>
<b>Area Commerciale e Marketing</b>	<b>Area Commerciale e Marketing</b>

**Service desk, application management,  
assistenza sistemistica**

**Service desk, application  
management, assistenza  
sistemistica**

In questa ottica organizzativa, quindi, un particolare ruolo viene attribuito al Responsabile Sistema di Gestione Integrato il quale riporta alla Direzione Generale le prestazioni del sistema di Gestione Integrato, realizzando l'integrazione delle procedure operative e delle tematiche trasversali ai servizi e ne verifica l'efficacia.

Tale apparato normativo interno, in tutt'uno con le certificazioni acquisite e mantenute dalla Società, implementano il MOG231 il quale, tramite i presidi di controllo definiti nelle parti speciali e i protocolli comportamentali, si integra con esso, elevando gli standard di controllo interno verso la conformità normativa voluta dal d.lgs.231/01.



Il ruolo delle certificazioni o dell'adesione volontaria alle norme tecniche internazionali, quali, ad esempio, ISO, ISO/IEC, oppure, a livello nazionale, quelle sviluppate dall'UNI/CEI, assumono per Infodata S.p.A. un alto valore regolamentare interno poiché è ritenuto che le stesse forniscano le direttive cui conformarsi affinché i processi decisionali siano seguiti su regole certe e, pertanto, non frutto di personalismi o esperienze pregresse.

Allo stesso tempo, in linea anche con gli intendimenti giurisprudenziali, l'adesione volontaria a tali norme, seppur costante e quotidiana fonte di ispirazione operativa, non può esser considerata quale una risorsa di deresponsabilizzazione sui ruoli e sui processi. È da dividerne, invece, il ruolo organizzativo di tali norme, che rappresentano una metodologia condivisa per ottimizzare le *performance* nell'ottica comune.

Questo significa che, nell'ambito dell'assetto organizzativo dettato con l'adozione del MOG231, strumentale alla prevenzione di condotte tipiche di natura sostanzialmente penale cagionate da un difetto organizzativo, l'adesione a tali schemi alimenta una consapevolezza maggiore ed una padronanza nei processi aziendali, tale da guidare le risorse di Infodata S.p.A. verso condotte cui conformarsi. L'effetto e l'utilità operativa riconosciuta dal vertice societario, attraverso anche le certificazioni, è quello di diffondere metodologie operative che non lasciano spazio a valutazioni o ad azioni che si discostino da quanto impresso nelle procedure aziendali, onde addivenire ad una gestione organizzata che possa evitare di esporre la Società a perdite o situazioni di rischio.

La Società ha strutturato un sistema di audit interno condotto da personale altamente qualificato e formato, al fine di specificare le modalità di esecuzione delle attività di programmazione, pianificazione e conduzione di azioni volte a migliorare le *performance* del proprio "SGS". Essi, basati su specifici obiettivi e regolati da specifiche procedure interne, alimentano il sistema di controlli interni attuati dalla Società al fine di prevenire condotte che possano divergere dagli scopi sociali, ovvero, arrecare pregiudizio alla stessa, tanto in termini legali quanto in termini di non conformità alle norme cui aderisce.

La Società ha sviluppato un insieme di strumenti di governo dell'organizzazione, che garantiscono il funzionamento della Società e di seguito sinteticamente indicati:

-  Statuto Sociale
-  Sistema di deleghe e procure

- Struttura gerarchico-funzionale (organigramma)
- Codice etico di Gruppo Infodata
- Codice etico e di comportamento Infodata S.p.A.
- Modello organizzativo di gestione e controllo ai sensi del d.lgs.231/01
- Istituzione dell'Organismo di Vigilanza
- Sistema di gestione delle segnalazioni Whistleblowing – PGSW
- Adozione di un sistema disciplinare 231
- Adesione a schemi di certificazione
- Definizione di un Sistema di Gestione Integrato – SGI
- Adesione ad un Sistema di Gestione Integrato di Gruppo – SGIG
- Definizione di procedure interne operative
- Programmazione di audit sul Sistema di Gestione Integrato – SGI
- Formazione delle risorse
- Adozione di sistemi informativi orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi utilizzati a supporto delle attività operative connesse al business.

### 3.1 Il sistema di gestione per la salute e sicurezza sul lavoro (SGSL)

Con lo scopo di definire ed adottare il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche ai sensi del d.lgs.231/01 previsto dal T.U.S.S.L., Infodata S.p.A. nel 2022 ha concluso il percorso di adeguamento alla norma UNI ISO 45001:2018 “*Sistemi di gestione per la salute e sicurezza sul lavoro – Requisiti e guida per l’uso*”.

Il sistema prevenzionistico definito con l’ottenimento della suddetta certificazione, rientra a pieno titolo tra le componenti del MOG 231 in adozione, strumentali a rafforzare la politica dell’ente in tema di salute e sicurezza nei luoghi di lavoro.

Allo stesso tempo, la prova dell’adempimento e la quotidiana attuazione di tutti gli obblighi giuridici previsti dall’art.30 del d.lgs.81/08, consente all’ente di innalzare i presidi cautelari strumentali ad evitare il verificarsi di uno dei reati presupposto previsti dall’art.25-*septies* del d.lgs.231/01.

## 4. La disciplina del decreto legislativo n.231 del 2001

### 4.1 Principi generali

In data 8 giugno 2001 è stato emanato il decreto legislativo n.231 (di seguito denominato “Decreto”), in attuazione della delega di cui all’art. 11 della L.29 settembre 2000 n.300, con il quale il legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche.

In particolare:

- alla Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee,
- alla Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri,
- alla Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali

stranieri nelle operazioni economiche ed internazionali.

Il Decreto, recante “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*”, ha introdotto nell’ordinamento giuridico italiano un regime di responsabilità amministrativa a carico degli enti (da intendersi come società, associazioni, consorzi, etc.) per reati tassativamente elencati e commessi nel loro interesse o vantaggio da:

- **persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli enti medesimi,**
- **persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.**

La responsabilità amministrativa dell’ente si aggiunge a quella della persona fisica, che ha commesso materialmente il reato: la previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti penali ivi espressamente previsti, gli Enti che abbiano tratto interesse e/o vantaggio dalla commissione del reato.

#### 4.2 Il contenuto del Decreto

Il provvedimento è diviso in IV Capi, ove al Capo I si individuano i principi generali e criteri di attribuzione della responsabilità amministrativa, le sanzioni e le fattispecie di reato che fondano tale responsabilità.

Il Decreto, sin dalla sua emanazione, ha visto negli anni incrementare le fattispecie di reato attraverso cui fondare una responsabilità in sede penale dell’ente. Invero, trattasi di un elenco tassativo di reati che, appunto, al fine di contrastare i fenomeni delittuosi aziendali, annovera differenti famiglie di reati, che prendono comunemente il nome di “*reati presupposto*”, in linea con le scelte di politica criminale di un Legislatore sempre al passo con le nuove esigenze repressive. Ad oggi, l’elenco è composto dalle seguenti fattispecie:

**Art.24.** *Indebita percezione di erogazioni, truffa in danno 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 pubbliche forniture;*

**Art.24-bis.** *Delitti informatici e trattamento illecito di dati;*

**Art.24-ter.** *Delitti di criminalità organizzata;*

**Art.25.** *Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d’ufficio;*

**Art.25-bis.** *Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;*

**Art.25-bis.1.** *Delitti contro l’industria e il commercio;*

**Art.25-ter.** *Reati societari;*

**Art.25-quater.** *Delitti con finalità di terrorismo o di eversione dell’ordine democratico;*

**Art.25-quater.1.** *Pratiche di mutilazione degli organi genitali femminili;*

**Art.25-quinquies.** *Delitti contro la personalità individuale;*

**Art.25-sexies.** *Abusi di mercato;*

**Art.25-septies.** *Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;*

**Art.25-octies.** *Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché*



autoriciclaggio;

**Art.25-octies.1** *Delitti in materia di strumenti di pagamento diversi dai contanti;*

**Art.25-novies.** *Delitti in materia di violazione del diritto d'autore;*

**Art.25-decies.** *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;*

**Art.25-undecies.** *Reati ambientali;*

**Art.25-duodecies.** *Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;*

**Art.25-terdecies.** *Razzismo e xenofobia;*

**Art.25-quaterdecies.** *Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati;*

**Art.25-quinquiesdecies.** *Reati tributari;*

**Art.25-sexiesdecies.** *Contrabbando;*

**Art.26.** *Delitti tentati.*

Al Capo II, vengono trattate le responsabilità dell'ente e le vicende modificative dello stesso.

Al Capo III, vengono trattate le norme relative al procedimento di accertamento ed applicazione delle sanzioni amministrative.

Al Capo IV, si rinvengono le disposizioni di attuazione e coordinamento.

#### 4.3 Il presupposto della punibilità dell'ente.

Il portato normativo del Decreto, per espressa previsione, si applica agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica; non si applica allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale. Gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Fermo restando il principio normativo in base al quale la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato o non è imputabile, o il reato si estingue per una causa diversa dall'amnistia, i criteri di imputazione del fatto-reato all'ente, si ritrovano nell'art.5 del Decreto.

## **Art.5 - Responsabilità dell'ente**

**Co.1.** *L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:*

*a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;*

*b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).*

**Co.2.** *L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi.*

Sotto un punto di vista soggettivo, il primo comma guarda ai vertici societari, ovvero, a quelle 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, (definiti anche come "apicali");

il secondo comma guarda a coloro i quali siano sottoposti alla direzione o alla vigilanza di uno dei soggetti in precedenza indicati, in ottemperanza all'art.5, co.1 lett. a) del Decreto, (definiti anche come "sottoposti").

Sotto il punto di vista oggettivo, invece, il Legislatore ha valutato un criterio su cui possa fondarsi la responsabilità dell'ente, ossia "*l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio*".

La prova della ricorrenza dell'interesse o del vantaggio per l'ente, appare quale punto di partenza per la rimproverabilità della condotta derivante da reato. Per l'individuazione delle nozioni di "interesse" e di "vantaggio", la nota pronunzia a Sezioni Unite n.38343 del 24/04/2014, P.G., R.C., Espenhahn e altri, Rv. 261114-01 e 261115-01, meglio nota come Sentenza ThyssenKrupp, definisce che tali criteri sono alternativi e concorrenti tra loro, in quanto il criterio dell'interesse esprime una valutazione teleologica del reato, apprezzabile "*ex ante*", cioè al momento della commissione del fatto e secondo un metro di giudizio marcatamente soggettivo, mentre quello del vantaggio ha una connotazione essenzialmente oggettiva, come tale valutabile "*ex post*", sulla base degli effetti concretamente derivati dalla realizzazione dell'illecito.

In tema di responsabilità da reato degli enti derivante da reati colposi di evento, invece, i criteri di imputazione oggettiva, rappresentati dal riferimento contenuto nel d.lgs.231 del 2001, art.5, all'interesse o al vantaggio, devono essere riferiti alla condotta e non all'evento. Interesse e vantaggio non costituiscono un'endiadi, essendo concetti giuridicamente diversi e potendosi ipotizzare un interesse prefigurato come discendente da un indebito arricchimento e magari non realizzato e, invece, un vantaggio obiettivamente conseguito tramite la commissione di un reato. Infine, l'ente non risponde se le persone indicate nel co.1 hanno agito nell'interesse esclusivo proprio o di terzi.

#### 4.4 La condizione esimente della responsabilità amministrativa dell'ente

##### 4.4.1 Primo profilo soggettivo: reato commesso da un soggetto posto in posizione apicale

L'art. 6 del Decreto stabilisce che l'ente non risponde del reato commesso da tale soggetto nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, "*modelli di organizzazione di gestione e controllo idonei a prevenire reati della specie di quello verificatosi*" (di seguito denominato "Modello/i" o "MOG").

Orbene, il Legislatore, qualora l'ente venga tratto a giudizio per rispondere, in sede penale, di un reato presupposto derivante da fatto altrui, al fine di mandare esente lo stesso dalla responsabilità amministrativa ex d.lgs.231/01, impone il verificarsi di determinate condizioni.

La verificabilità di tutte le condizioni imposte all'art.6 del Decreto, rappresentano il grado di responsabilizzazione del vertice societario nel dotare l'ente di una chiara politica organizzativa improntata sul rispetto della legalità.

Trattasi, invero, di una espressione tipica del portato normativo del decreto che prevede, appunto, la dimostrazione di una assenza di "*colpa organizzativa*" e, quindi, la definizione di un assetto interno basato su elementi idonei ad evitare il verificarsi di eventi delittuosi, "*presupposto*" della responsabilità amministrativa dell'ente.

Nel perimetro della verificabilità dell'efficacia della politica preventiva assunta dall'ente, il

Legislatore ha voluto calibrare l'onere probatorio, a seconda che il reato fosse stato commesso "nell'interesse o a vantaggio dell'ente" da quei soggetti che rivestono posizioni c.d. di "apicali" o di "sottoposti".

## **Art.6 - Soggetti in posizione apicale e modelli di organizzazione dell'ente**

**Co.1:** *Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che:*

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

Se, quindi, il reato è stato commesso da soggetti "apicali" che, cioè, 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, vige il principio in base al quale grava sulla pubblica accusa l'onere di dimostrare l'esistenza dell'illecito dell'ente, mentre a quest'ultimo incombe l'onere, con effetti liberatori, di dimostrare di aver adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi l'ente.

L'efficacia esimente e, quindi, la possibilità per l'ente di veder esclusa la responsabilità amministrativa derivante da reato per fatto altrui, passa in prima istanza attraverso **la prova dell'adozione ed efficace attuazione del MOGC idoneo.**

A tale prima condizione devono seguire:

- l'affidamento e il riconoscimento di poteri di vigilanza e controllo ad un organismo dell'ente che entrerà a pieno titolo tra i vertici aziendali, a cui la legge attribuisce un ruolo di particolare importanza affianco al vertice amministrativo - di *staff* - nel corso dell'attuazione, monitoraggio e aggiornamento del MOG 231: l'Organismo di Vigilanza o ODV;
- la prova che il reato è stato commesso perché risultato dell'elusione delle prescrizioni imposte dal MOG da parte degli apicali, ovvero sia un atteggiamento che, al pari di una frode, deve consistere in una condotta ingannevole, falsificatrice, obliqua, subdola, ovvero di aggiramento di una norma imperativa non essendo sufficiente, invece, la semplice violazione della stessa;
- la prova che l'ODV sia stato efficace nella sua azione di vigilanza e controllo, nell'applicazione di quanto prescritto nel MOG all'interno dell'ente.

### 4.4.2 Il contenuto del Modello organizzativo di gestione e controllo a fini esimenti.

Onde veder riconosciuta efficacia pratica al MOG e, quindi, consentire allo stesso l'esplicazione degli effetti organizzativi tipici adottati dall'Organo di vertice, per espressa previsione normativa esso deve rispondere a determinate esigenze:

**Co.2:** *In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze:*

- a) individuare le attività nel cui ambito possono essere commessi reati;
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Tali requisiti, sopperiscono appunto all'esigenza di manifestare la politica organizzativa dell'ente cioè come lo stesso intende governare il rischio che nell'ambito della sua struttura possano esser commessi determinati reati e, qualora commessi, l'ente possa trarne un interesse o un vantaggio. Il MOG di Infodata S.p.A. è stato elaborato seguendo quanto imposto dall'art.6, co.2 del Decreto, come meglio descritto nel paragrafo dedicato al Progetto 231 della Società.

I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al co.2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati. Nella redazione del presente MOG, si è tenuto in debito conto quanto previsto dalle Linee Guida di Confindustria - *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo, Ult. Ed.* -, il *Co So Report Framework*, la norma UNI-ISO 31000:2018 in tema di Linee guida per la gestione del rischio e di quelle adottate dalla Società su cui si basa il Sistema di Gestione Integrato interno. Sono, pertanto, state effettuate delle azioni che hanno coinvolto tutti i livelli della Società, al fine di soddisfare quanto richiesto a livello normativo che hanno portato:

- all'individuazione delle aree a rischio ove potenzialmente potessero esser commessi reati;
- ad una armonizzazione dei processi interni in linea con un'accresciuta consapevolezza in termini di prevenzione del reato presupposto, tramite rafforzamento degli stessi mediante protocolli di condotta previsti nelle singole sezioni di Parte Speciale;
- definizione di prerogative nell'uso degli strumenti e flussi finanziari;
- apertura di un canale informativo verso l'OdV caratterizzato da flussi idonei a presidiare le fonti di rischio, in grado, altresì, di coinvolgere tale organo nella costante applicazione interna del MOG all'indirizzo: [odv\\_inf@infodata.net](mailto:odv_inf@infodata.net);
- rafforzamento del sistema disciplinare interno, che vede oggi anche il MOG di Infodata S.p.A. quale ulteriore fonte normativa disciplinare e regolamentare, che si affianca a quello nazionale.

#### 4.4.3 Il sistema di gestione delle segnalazioni di illecito di Infodata S.p.A.

Con il d.lgs.24/2023 recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali", Infodata S.p.A. ha adeguato il proprio assetto gestionale deputato alla ricezione delle segnalazioni di illecito, c.d. "whistleblowing".

La Società, previa attivazione del nuovo canale di segnalazione interno per ricevere segnalazioni scritte, si è dotata di un nuovo assetto di *governance* nonché di nuove procedure atte a definire il proprio sistema di gestione delle segnalazioni. Tutta la documentazione riferibile a tale sistema

di gestione è parte integrante del presente MOG 231, ed è codificata con il codice PGSW e definisce, oltre agli aspetti gestionali, le modalità tramite cui i soggetti legittimati dalla legge possono inoltrare segnalazioni ed esser garantito loro tale diritto.

***Cosa è possibile segnalare.***

Collegandosi al sito [www.infodata.net](http://www.infodata.net), nella sezione dedicata è possibile effettuare segnalazioni di informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria intrattiene un rapporto giuridico lavorativo, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni, relativamente a:

- reati presupposto, ai sensi del d.lgs.231/01;
- violazioni del MOG 231 di Infodata S.p.A.;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al d.lgs.24/2023 ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al decreto, relativi ai specifici settori;
- atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
- atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nel decreto.

L'elenco è da considerarsi tassativo.

In via alternativa e nel rispetto delle condizioni imposte dal d.lgs.24/2023, la persona segnalante possono ricorrere al canale esterno di segnalazione attivato e gestito dall'Autorità Nazionale Anticorruzione (ANAC), collegandosi al sito <https://www.anticorruzione.it/-/whistleblowing> e seguire le istruzioni di compilazione del modulo predisposto dall'Autorità.

La persona segnalante, inoltre, può effettuare una divulgazione pubblica, qualora ne ricorrano le condizioni previste dalla legge o rivolgersi all'autorità giudiziaria. In entrambi i casi di divulgazione pubblica o denuncia all'autorità giudiziaria, essi godranno sempre della medesima protezione riconosciuta alla persona segnalante.

***Cosa non è possibile segnalare.***

Non è possibile segnalare le notizie palesemente prive di fondamento, doglianze personali, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio).

***Chi può segnalare.***

Le segnalazioni possono esser effettuate solo ed esclusivamente da chi ritiene di aver appreso

informazioni sulle violazioni segnalabili nell'ambito del contesto lavorativo di Infodata S.p.A. Ci si riferisce, dunque, a soggetti che abbiano intrattenuto con la società attività lavorative (dipendenti, tirocinanti, volontari, candidati o quando il rapporto è concluso) o professionali (consulenti, fornitori anche in fase precontrattuale), presenti o passate, attraverso le quali, indipendentemente dalla natura di tali attività, abbia acquisito informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria. Stessa facoltà è concessa a gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza.

Infodata S.p.A. riconosce le medesime garanzie e misure di protezione anche a determinate categorie di soggetti legati al segnalante da un determinato rapporto e, cioè, ai facilitatori; alle persone del medesimo contesto lavorativo che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado; ai colleghi di lavoro che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente; agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo.

#### 4.5 Secondo profilo soggettivo: reato commesso da soggetti "sottoposti".

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza di obblighi di direzione e vigilanza.

## **Art.7 - Soggetti sottoposti all'altrui direzione e modelli di organizzazione dell'ente**

**Co.1.** *Nel caso previsto dall'articolo 5, comma 1, lettera b), l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.*

**Co.2.** *In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.*

**Co.3.** *Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.*

**Co.4.** *L'efficace attuazione del modello richiede:*

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

Detta inosservanza è, in ogni caso, esclusa qualora l'ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Tali MOG devono prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

Tutto questo, però, passa inevitabilmente per una preventiva adozione e successiva efficace attuazione del modello che richiede, qualora adottato:



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

Tale criterio di imputazione impone un diverso approccio probatorio in fase giudiziale: trattasi, invero, di un onere che ricade completamente sulla pubblica accusa di provare la tenuta del MOG adottato dalla società. Partendo, quindi, da una situazione in cui l'ente abbia preventivamente adottato un proprio Modello, l'onere probatorio deve esser rivolto verso l'emersione di quegli indici di inosservanza degli obblighi di direzione e vigilanza impartiti al dipendente.

In tale ipotesi per ascrivere all'ente una responsabilità per un reato commesso da subordinati, è necessario che un rimprovero possa essere mosso ai vertici, e questo consegue nella fattispecie, per l'appunto, alla inosservanza degli obblighi di direzione o vigilanza. Trattasi, invero, di una responsabilità colposa dei vertici per non aver impedito un reato doloso o colposo la cui commissione è legata all'inosservanza di detti obblighi.

In definitiva, gli elementi costitutivi dell'illecito dell'ente in questione sono, dunque:

- un reato commesso da un sottoposto ancorché non identificato;
- il perseguimento con il reato dell'interesse (parziale o esclusivo) dell'ente;
- che la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza da parte dei vertici (elemento, quest'ultimo, aggiuntivo rispetto alla responsabilità da reato dei vertici per le ragioni già individuate).

#### 4.6 L'apparato sanzionatorio

Il Decreto prevede un apparato sanzionatorio proprio, definito dalla Sezione II.

Esso consta di sanzioni amministrative connesse all'accertamento giudiziale del fatto-reato rientrante nello schema tassativamente individuato dal legislatore.

Le sanzioni per gli illeciti amministrativi dipendenti da reato sono:

- a. la sanzione pecuniaria;
- b. le sanzioni interdittive;
- c. la confisca;
- d. la pubblicazione della sentenza.

In merito alle sanzioni interdittive, sono previste:

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

#### **La sanzione pecuniaria – Artt.10, 11, 12**

Per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria. Essa viene applicata per quote in un numero non inferiore a cento né superiore a mille. L'importo di una quota va da un minimo di euro 258 (lire cinquecentomila) ad un massimo di euro 1.549 (lire

tre milioni) e non è ammesso il pagamento in misura ridotta.

Nella commisurazione della sanzione pecuniaria il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione.

In determinati casi, la sanzione pecuniaria è ridotta della metà o da un terzo alla metà o dalla metà ai due terzi:

- **riduzione della metà:**

- a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- b) il danno patrimoniale cagionato è di particolare tenuità.

In tali casi, l'importo della quota è sempre di euro 103 (lire duecentomila).

- **riduzione da un terzo alla metà** se, prima della dichiarazione di apertura del dibattimento di I° grado:

- a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

- **riduzione dalla metà ai due terzi:**

- a) nel caso in cui concorrono entrambe le condizioni previste dalle lettere riferite alla riduzione da un terzo alla metà, la sanzione è ridotta dalla metà ai due terzi.

In ogni caso, la sanzione pecuniaria non può essere inferiore a euro 10.329 (lire venti milioni).

### **Le sanzioni interdittive – Artt.13, 14, 23**

Sono applicate in relazione ai reati per i quali sono espressamente previste e quando ricorre almeno una delle seguenti condizioni:

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

Hanno una durata non inferiore a tre mesi e non superiore a due anni, salvo diversa disposizione e non si applicano quando l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo, oppure qualora il danno patrimoniale cagionato è di particolare tenuità.

Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente. Il giudice ne determina il tipo e la durata sulla base dei criteri indicati nell'articolo 11, del Decreto, tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso.

La sanzione del divieto di contrattare con la pubblica amministrazione può anche essere limitata a determinati tipi di contratto o a determinate amministrazioni. L'interdizione dall'esercizio di un'attività comporta la sospensione ovvero la revoca delle autorizzazioni, licenze o concessioni funzionali allo svolgimento dell'attività.



Se necessario, le sanzioni interdittive possono essere applicate congiuntamente.

L'interdizione dall'esercizio dell'attività si applica soltanto quando l'irrogazione di altre sanzioni interdittive risulta inadeguata. Può essere disposta l'interdizione definitiva dall'esercizio dell'attività se l'ente ha tratto dal reato un profitto di rilevante entità ed è già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività. Il giudice può applicare all'ente, in via definitiva, la sanzione del divieto di contrattare con la pubblica amministrazione ovvero del divieto di pubblicizzare beni o servizi quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità è sempre disposta l'interdizione definitiva dall'esercizio dell'attività e non si applicano le disposizioni previste in tema di riparazione delle conseguenze del reato, di cui all'art.17. Trattasi, queste, di condizioni che escludono l'applicazione delle interdittive quando, prima della dichiarazione di apertura del dibattimento di I° grado, concorrono le seguenti condizioni:

- a. l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- b. l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi;
- c. l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Chiunque, nello svolgimento dell'attività dell'ente a cui è stata applicata una sanzione o una misura cautelare interdittiva trasgredisce agli obblighi o ai divieti inerenti a tali sanzioni o misure, è punito con la reclusione da sei mesi a tre anni. Nei confronti dell'ente nell'interesse o a vantaggio del quale il reato è stato commesso, si applica la sanzione amministrativa pecuniaria da duecento e seicento quote e la confisca del profitto. Se dal reato di cui al comma 1, l'ente ha tratto un profitto rilevante, si applicano le sanzioni interdittive, anche diverse da quelle in precedenza irrogate.

### **Commissario giudiziale – Art.15**

Se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- a. l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- b. l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Con la sentenza che dispone la prosecuzione dell'attività, il giudice indica i compiti ed i poteri del commissario, tenendo conto della specifica attività in cui è stato posto in essere l'illecito da parte dell'ente. Nell'ambito dei compiti e dei poteri indicati dal giudice, il commissario cura l'adozione e l'efficace attuazione dei modelli di organizzazione e di controllo idonei a prevenire reati della specie di quello verificatosi. Non può compiere atti di straordinaria amministrazione senza

autorizzazione del giudice. Il profitto derivante dalla prosecuzione dell'attività viene confiscato. La prosecuzione dell'attività da parte del commissario non può essere disposta quando l'interruzione dell'attività consegue all'applicazione in via definitiva di una sanzione interdittiva.

#### **Pubblicazione della sentenza di condanna – Art.18**

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva. Avviene ai sensi dell'articolo 36 del codice penale nonché mediante affissione nel comune ove l'ente ha la sede principale. La pubblicazione della sentenza è eseguita, a cura della cancelleria del giudice, a spese dell'ente.

#### **Confisca – Art.19**

Nei confronti dell'ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede. Quando non è possibile eseguire la confisca a norma del comma 1, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato. Tale ipotesi di confisca per equivalente è espressamente prevista qualora sia stato accertato che l'ente abbia tratto un interesse o un vantaggio illecito dalla commissione di un fatto-reato da parte di soggetti in posizione apicale.

#### **5. Il fenomeno del Gruppo di società e l'applicazione del d.lgs.231/01**

La presente trattazione appare di fondamentale importanza in virtù della struttura del Gruppo Infodata e del ruolo di capogruppo assunto dalla società Infodata S.p.A.

Il sistema degli illeciti amministrativi dipendenti da reato è fondato su un ente singolarmente considerato ed ignora il fenomeno dei gruppi di società, ovvero dell'aggregazione di una pluralità di società che operano sotto la direzione ed il controllo strategico ed unitario di una capogruppo. Le singole società facenti parte di un Gruppo costituiscono entità autonome ed indipendenti, ciascuna dotata di una propria soggettività giuridica: sono tra loro coordinate e sottoposte al controllo economico-strategico da parte di un unico soggetto che le governa e le condiziona secondo un indirizzo gestionale unitario, al fine di attuare un programma comune ed ulteriore rispetto a quello realizzabile attraverso le singole imprese.

Né discende che questo fenomeno, non può essere considerato alla stregua di un "ente" e, dunque, non costituisce diretto centro di imputazione della responsabilità da reato, non essendo inquadrabile tra i soggetti indicati dall'art.1 del Decreto: in altri termini, non appare in alcun modo configurabile una responsabilità diretta del Gruppo ai sensi del d.lgs.231/01.

È possibile, però, che le singole entità che fanno parte del Gruppo possano esser imputate ai sensi del Decreto, ricorrendone le condizioni di legge.

In costanza di tale aggregazione di imprese, di fondamentale importanza appare delineare le conseguenze connesse alla propagazione della responsabilità da una società ad altre appartenenti al medesimo Gruppo.

Questi i possibili scenari:

- responsabilità della capogruppo per il reato commesso nell'interesse o a vantaggio della controllata (c.d. responsabilità ascendente);
- della responsabilità della controllata per il reato commesso nell'interesse o a vantaggio della capogruppo e della controllata per il reato commesso nell'interesse od a vantaggio di altra

controllata (c.d. responsabilità discendente).

Onde addivenire ad una rappresentazione chiara del fenomeno dei gruppi societari nell'abito del d.lgs.231/01, vengono di seguito espressi principi normativi guida generali ritenuti indispensabili al fine di poter meglio comprendere i passaggi che oggi consentono l'applicazione della Decreto alla disciplina dei gruppi:

#### Codice civile

---

#### **Art.2359 – Società controllate e società collegate**

Sono considerate società controllate:

- 1) le società in cui un'altra società dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria;
- 2) le società in cui un'altra società dispone di voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria;
- 3) le società che sono sotto influenza dominante di un'altra società in virtù di particolari vincoli contrattuali con essa.

Ai fini dell'applicazione dei numeri 1) e 2) del primo comma si computano anche i voti spettanti a società controllate, a società fiduciarie e a persona interposta: non si computano i voti spettanti per conto di terzi.

Sono considerate collegate le società sulle quali un'altra società esercita un'influenza notevole. L'influenza si presume quando nell'assemblea ordinaria può essere esercitato almeno un quinto dei voti ovvero un decimo se la società ha azioni quotate in mercati regolamentati.

#### **Capo IX – Direzione e coordinamento di società**

#### **Art.2497 – Responsabilità**

Le società o gli enti che, esercitando attività di direzione e coordinamento di società, agiscono nell'interesse imprenditoriale proprio o altrui in violazione dei principi di corretta gestione societaria e imprenditoriale delle società medesime, sono direttamente responsabili nei confronti dei soci di queste per il pregiudizio arrecato alla redditività ed al valore della partecipazione sociale, nonché nei confronti dei creditori sociali per la lesione cagionata all'integrità del patrimonio della società. Non vi è responsabilità quando il danno risulta mancante alla luce del risultato complessivo dell'attività di direzione e coordinamento ovvero integralmente eliminato anche a seguito di operazioni a ciò dirette.

Risponde in solido chi abbia comunque preso parte al fatto lesivo e, nei limiti del vantaggio conseguito, chi ne abbia consapevolmente tratto beneficio.

Il socio ed il creditore sociale possono agire contro la società o l'ente che esercita l'attività di direzione e coordinamento, solo se non sono stati soddisfatti dalla società soggetta alla attività di direzione e coordinamento. Nel caso di fallimento, liquidazione coatta amministrativa e amministrazione straordinaria di società soggetta ad altrui direzione e coordinamento, l'azione spettante ai creditori di questa è esercitata dal curatore o dal commissario liquidatore o dal commissario straordinario.

#### **Art.2497-sexies – Presunzioni**

Ai fini di quanto previsto nel presente capo, si presume salvo prova contraria che l'attività di direzione e coordinamento di società sia esercitata dalla società o ente tenuto al consolidamento dei loro bilanci o che comunque le controlla ai sensi dell'articolo 2359.

#### **Art.2497-septies – Coordinamento fra società**

Le disposizioni del presente capo si applicano altresì alla società o all'ente che, fuori dalle ipotesi di cui all'articolo 2497 sexies, esercita attività di direzione e coordinamento di società sulla base di un contratto con le società medesime o di clausole dei loro statuti.

---

**D.lgs. 9 aprile 1991, n. 127 - Attuazione delle Direttive n. 78/660/CEE e n. 83/349/CEE in materia societaria, relative ai conti annuali e consolidati, ai sensi dell'art. 1, comma 1, della legge 26 marzo 1990, n. 69.**

---

#### **Art. 25 – Imprese obbligate a redigere il bilancio consolidato**

1. Le società per azioni, in accomandita per azioni, e a responsabilità limitata che controllano un'impresa debbono

redigere il bilancio consolidato secondo i criteri stabiliti dalle disposizioni degli articoli seguenti.

2. Lo stesso obbligo, hanno gli enti di cui all'art. 2201 del codice civile, le società cooperative e le mutue assicuratrici che controllano una società per azioni, in accomandita per azioni o a responsabilità limitata.

#### **Art. 26 - Imprese controllate**

1. Agli effetti dell'art. 25 sono considerate imprese controllate quelle indicate nei numeri 1) e 2) del primo comma dell'art. 2359 del codice civile.

2. Agli stessi effetti sono in ogni caso considerate controllate:

a. le imprese su cui un'altra ha il diritto, in virtù di un contratto o di una clausola statutaria, di esercitare un'influenza dominante, quando la legge applicabile consenta tali contratti o clausole;

b. le imprese in cui un'altra, in base ad accordi con altri soci, controlla da sola la maggioranza dei diritti di voto.

3. Ai fini dell'applicazione del comma precedente si considerano anche i diritti spettanti a società controllate, a società fiduciarie e a persone interposte; non si considerano quelli spettanti per conto di terzi.

#### **5.1 Responsabilità della controllata per i reati commessi da soggetti appartenenti alla capogruppo**

In virtù del fatto che la controllata, in ottemperanza al citato art.2359 c.c., sia soggetta alla "direzione e controllo" della controllante e, quindi, parte di una più ampia dinamica industriale di aggregazione, imporrebbe di ritenere un'automatica responsabilizzazione della controllata per i reati commessi da soggetti funzionalmente collegati alla controllante e nell'esclusivo interesse o vantaggio di tali società.

Tale automatismo è stato sconfessato dalla giurisprudenza di legittimità (Cass. pen., Sez. VI, sent. n. 2658 del 2014), ritenendo la impossibilità di imputare la responsabilità da reato alle società controllate sulla scorta della mera esistenza del rapporto di controllo o di collegamento all'interno di un Gruppo societario, precisando, altresì, la necessità, ai fini della attribuzione di tale responsabilità, di verificare la ricorrenza in concreto dei criteri di imputazione della responsabilità da reato anche in capo a tali società.

#### **5.2 Responsabilità della controllante per i reati commessi da soggetti appartenenti alla organizzazione della controllata**

La direzione unitaria attribuita alla capogruppo, si sostanzia nell'esercizio dell'attività di "direzione e coordinamento" nei confronti delle società eterodirette; una pluralità sistematica e costante di atti di indirizzo idonei ad incidere sulle decisioni gestorie dell'impresa, cioè sulle scelte strategiche ed operative di carattere finanziario, industriale, commerciale che attengono alla conduzione degli affari sociali.

Su tali basi, non basta e non è consentito guardare ad un interesse globale, il c.d. "interesse di gruppo", per poter configurare una responsabilità della capogruppo *ex d.lgs.231/01*. Tale definizione non si rinviene nel Decreto ed è concepito come veicolo di realizzazione mediata dell'oggetto sociale ove la società capogruppo assume un ruolo indubbiamente invasivo e di influenza in base all'attività di direzione e coordinamento sulle controllate e, per tale motivazione, destinataria anche di probabili vantaggi illeciti.

Non è possibile, però imputare alla società controllante la responsabilità per i reati commessi nell'ambito delle società controllate, unicamente sulla scorta del dato relativo alla appartenenza della società ad un Gruppo. Tale appartenenza, infatti, non sempre implica necessariamente che le scelte compiute dalla controllata perseguano un interesse che trascende quello proprio per coincidere con un interesse più ampio, riferibile, appunto, all'intero raggruppamento di imprese

o alla società capogruppo.

La presenza di un Gruppo societario non legittima per ciò solo qualsivoglia condotta di asservimento di una società all'interesse delle altre società del Gruppo, dovendosi, per contro, ritenere che l'autonomia soggettiva e patrimoniale che contraddistingue ogni singola società imponga all'amministratore di perseguire prioritariamente l'interesse della specifica società cui sia preposto e, pertanto, di non sacrificarne l'interesse in nome di un diverso interesse, ancorché riconducibile a quello di chi sia collocato al vertice del gruppo, che non procurerebbe alcun effetto a favore dei terzi creditori dell'organismo impoverito (Cass. pen., sez. V, sent. del 08/11/2007, n. 7326, Belleri, Rv.239108).

La giurisprudenza (Cass. pen, sez. V, sent. del 18/01/2011, n.24583, Tosinvest, Rv. 249820, ribadito anche da Cass. pen., sez. V, sent. del 29/01/2013, n.4324, UNIPOL G.F. S.p.A., Rv.254324) ha ritenuto che, ai fini della configurabilità della responsabilità di una holding ai sensi del d.lgs. 231/2001, è necessario che sussistano tre condizioni. Il primo requisito è che sia stato commesso uno dei reati di cui al citato Decreto. Il secondo elemento è che il reato presupposto sia stato commesso da una persona fisica che abbia con l'Ente rapporti di tipo organizzativo-funzionale; è cioè necessario che l'agente rivesta una posizione qualificata all'interno dell'ente. La terza condizione richiesta è che il reato presupposto sia stato commesso nell'interesse o a vantaggio dell'ente, interesse e vantaggio che devono essere verificati in concreto, dovendo la società ricevere una potenziale o effettiva utilità, ancorché non necessariamente di carattere patrimoniale, derivante dalla commissione del reato presupposto.

La società capogruppo o altre società facenti parte di un Gruppo possono essere chiamate a rispondere, ai sensi del d.lgs. n. 231 del 2001, del reato commesso nell'ambito dell'attività di una società controllata appartenente al medesimo Gruppo, purché nella consumazione del reato presupposto concorra anche almeno una persona fisica che agisca per conto della "holding" stessa o dell'altra società facente parte del Gruppo, perseguendo anche l'interesse di queste ultime, non essendo sufficiente – per legittimare un'affermazione di responsabilità ai sensi del d.lgs. n. 231 del 2001 della capogruppo o di altra società appartenente ad un medesimo gruppo – l'enucleazione di un generico riferimento al gruppo, ovvero ad un c.d. generale «interesse di gruppo».

Questo orientamento porta a ritenere che la capogruppo o altre società del Gruppo possono rispondere ai sensi del d.lgs.231, ma è necessario un coinvolgimento del soggetto che agisce per conto delle stesse e del soggetto che commette il reato.

Sul punto poi del c.d. "interesse di gruppo", spartiacque per l'imputazione 231, bisogna considerare che in una situazione di aggregazione di imprese una di queste può, attraverso la consumazione del reato, perseguire un proprio interesse anche quando il risultato si traduca in un vantaggio per un'altra componente dell'aggregato o, nell'immediato, nel soddisfacimento di un interesse particolare di quest'ultima. Trattasi, invero, non di un indistinto "interesse di gruppo", ma un coacervo di interessi che trovano semmai nella dinamica del Gruppo una attuazione unitaria attraverso la consumazione del reato. Per tale ragione nulla, infatti, legittima la presunzione della coincidenza dell'interesse di Gruppo con quello immediato delle singole società controllate: occorrerà sempre una attenta disamina delle circostanze del caso concreto, onde

verificare se, effettivamente, la controllante abbia avuto interesse o tratto vantaggio dall'azione della singola controllata.

In definitiva, quindi, è ammissibile una responsabilità, ai sensi d.lgs.231 del 2001, della società capogruppo per reati commessi nell'ambito dell'attività delle società da essa controllate a condizione che a) il soggetto che agisce per conto della capogruppo concorra con il soggetto che commette il reato per conto della persona giuridica controllata; b) possa ritenersi che la capogruppo abbia ricevuto un concreto vantaggio o perseguito un effettivo interesse a mezzo del reato commesso nell'ambito dell'attività svolta da altra società (Cass. pen., sez. II, sent. del 27/09/2016, n.52316, Riva, Rv. 268960).

### 5.3 I modelli organizzativi nell'ambito dei gruppi

Nell'ottica dei principi normativi connessi al fenomeno del Gruppo di società, i modelli di organizzazione e gestione della capogruppo e delle controllate dovrebbero, pertanto, opportunamente adottare misure organizzative intese ad evitare l'asservimento delle controllate al risultato economico della capogruppo mediante la commissione di delitti presupposto.

Con riferimento ai gruppi di società, quindi, che ciascuna di esse, ovvero sia la capogruppo che le controllate, ha l'onere di adottare un autonomo ed adeguato modello organizzativo, a prescindere dall'opportunità, evidenziata anche dalla dottrina, di coordinare le varie iniziative assunte al riguardo (Cass. pen., sez. II, sent. del 27/09/2016, n.52316, Riva, Rv. 268960).

## 6. Organismo di Vigilanza

### 6.1 I requisiti

L'art.6, co.1, lett.b), del d.lgs.231/01, individua l'istituzione di un Organismo di Vigilanza, come uno dei requisiti affinché l'ente possa essere esonerato dalla responsabilità "amministrativa" dipendente dalla commissione dei reati specificati nel Decreto stesso.

I requisiti che l'organismo di controllo deve soddisfare per un efficace svolgimento delle predette funzioni sono:

- **autonomia e indipendenza:** l'Organismo di Vigilanza deve essere sprovvisto di compiti operativi interni di amministrazione, gestione, esecutivi e/o operativi interni o comunque assimilabili allo schema del rapporto di lavoro dipendente subordinato e deve rappresentarsi come un organo di *staff* - come meglio si dirà in seguito - con il vertice amministrativo aziendale;
- **professionalità nell'espletamento dei suoi compiti istituzionali:** a tal fine il/i componente/i del suddetto organismo, deve/devono possedere conoscenze specifiche in materia in relazione alla realtà da vigilare, i reati presupposto, nonché qualsiasi tecnica utile per prevenire la commissione di reati, per scoprire quelli già commessi e individuarne le cause, nonché per verificare il rispetto dei modelli da parte degli appartenenti all'organizzazione aziendale;
- **onorabilità:** a tal fine il/i componente/i che rivestirà/anno tale carica non dovrà/anno trovarsi:
  - a) in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
  - b) non siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n.1423 o della legge 31 maggio 1965, n.575, e successive modificazioni ed integrazioni, salvi gli effetti della riabilitazione;
  - c) non abbiano procedimenti penali pendenti o riportato condanne penali di alcun tipo, salvi gli effetti



della riabilitazione.

Dovrà/anno possedere, inoltre, qualità personali quali alta moralità, integrità e condividere, con propria condotta irreprensibile, i valori e i principi etici dell'ente in vigilanza.

- **assenza di conflitti di interesse:** capaci di comprometterne l'indipendenza nell'azione di vigilanza;
- **continuità di azione:** al fine di garantire la costante attività di monitoraggio e di aggiornamento del Modello e la sua variazione al mutare delle condizioni aziendali di riferimento.

## 6.2 Composizione e individuazione

L'Organismo di Vigilanza può esser composto da membri interni e/o esterni alla compagine societaria. Tale composizione può raggruppare o meno diverse categorie di soggetti, selezionati opportunamente per il loro profilo accademico, le loro competenze e capacità a governare l'attuazione del MOG una volta approvato dall'organo di vertice.

Per tale via, la scelta, che ricade solo sul vertice societario di prediligere un Organismo a forma monocratica o collegiale (che racchiuda, in questa ultima ipotesi membri interni o membri esterni), deve, nella sostanza, riferirsi ad indici concreti, connessi all'attuale struttura organizzativa adottata dalla Società, alle capacità ed esperienza del/i membro/i che comporranno l'Organismo, al ruolo di vigilanza dello stesso connesso agli indici di rischio connessi all'attività sociale.

Il Consiglio di Amministrazione è chiamato a garantire la presenza dei requisiti sopra menzionati, valutare periodicamente l'adeguatezza dell'Organismo di Vigilanza in termini di struttura organizzativa e di poteri conferiti, apportando le modifiche e/o le integrazioni ritenute necessarie. L'Organismo di Vigilanza è configurato come unità di *staff* in posizione verticistica, riportando direttamente al solo Consiglio di Amministrazione. Una volta entrato in possesso dei poteri ad esso conferito dalla legge, ovvero a seguito di delibera istitutiva di tale organismo in forma monocratica o collegiale, il funzionamento di tale "organismo dell'ente" è disciplinato da un apposito "Regolamento", predisposto dall'Organismo medesimo, in virtù della sua autonomia operativa, ed ufficializzato nella seduta di insediamento al Consiglio di Amministrazione. Tale Regolamento, definisce l'agire dell'Organismo durante il periodo di reggenza della carica e, nello specifico, in ottemperanza a quanto previsto dall'art.6, co.1, lett.b), del d.lgs.231/01, la modalità di esercizio e gestione degli "autonomi poteri di iniziativa e controllo" ad esso riconosciuti; prevede, tra l'altro, le funzioni, i poteri e i doveri dell'Organismo, nonché la diramazione dei flussi informativi verso il CDA. Sotto questo profilo è previsto che ogni attività dell'Organismo di Vigilanza sia documentata per iscritto ed ogni riunione o ispezione cui esso partecipi sia opportunamente verbalizzata.

## 6.3 Nomina dell'OdV Infordata S.p.A.

Il Consiglio di Amministrazione di Infordata S.p.A. provvede alla nomina dell'Organismo di Vigilanza, definendo l'assetto, il periodo di durata della carica nonché l'assegnazione del *budget* di funzionamento che sarà gestito in autonomia dall'Organismo secondo quanto stabilito nel proprio Regolamento. L'OdV, infatti, deve disporre di adeguate risorse finanziarie al fine di garantire e rendere concreto l'autonomo potere di iniziativa e di controllo. L'ammontare del

*budget* in dotazione all'OdV deve essere sempre indicato nel verbale di nomina.

In relazione alla realtà di riferimento e ai rischi sottesi alla propria attività imprenditoriale, in fase di prima approvazione del MOG la Società ha deciso di dotarsi di un Organismo a composizione monocratica, affidando l'incarico ad un soggetto esterno di comprovata esperienza, valutata sulla compresenza dei requisiti sopra indicati, nonché, il livello tecnico, il *curriculum* accademico e professionale, conoscenza della società, onorabilità personale e professionale.

#### 6.4 Funzioni e poteri dell'Organismo di Vigilanza

In ossequio a quanto previsto dal Decreto, le funzioni svolte dall'Organismo di Vigilanza possono essere così riepilogate:

- vigilanza sull'effettività del Modello, che consiste nel verificare la coerenza tra comportamenti concreti e Modello istituito;
- valutazione dell'adeguatezza del Modello, ossia della idoneità dello stesso, in relazione alla tipologia di attività e alle caratteristiche dell'impresa, a ridurre ad un livello accettabile i rischi di realizzazione di reati. Ciò impone un'attività di aggiornamento dei modelli sia alle mutate realtà organizzative aziendali, sia ad eventuali mutamenti della legge in esame. L'aggiornamento può essere proposto dall'Organismo di Vigilanza, ma deve essere adottato - come già ricordato - dall'Organo amministrativo.

In particolare e a titolo meramente indicativo, i compiti dell'Organismo di Vigilanza sono così definiti:

1. vigilare sull'effettività del Modello attuando le procedure di controllo previste;
2. verificare l'efficacia nel prevenire i comportamenti illeciti;
3. verificare il mantenimento, nel tempo, dei requisiti richiesti promuovendo, qualora necessario, il necessario aggiornamento;
4. promuovere e contribuire, in collegamento con le altre unità interessate, all'aggiornamento e adeguamento continuo del Modello e del sistema di vigilanza sull'attuazione dello stesso;
5. assicurarsi i flussi informativi di competenza;
6. assicurare l'attuazione degli interventi di controllo programmati e non programmati;
7. segnalare alle funzioni competenti la notizia di violazione del Modello e monitorare l'applicazione delle sanzioni disciplinari.

Nell'espletamento delle sue funzioni, l'Organismo di Vigilanza ha la facoltà di:

1. emanare disposizioni intese a regolare l'attività dell'Organismo di Vigilanza;
2. accedere a qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo di Vigilanza ai sensi del d.lgs.231/01;
3. ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
4. disporre che i Responsabili delle funzioni aziendali forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello.

Nell'ambito del sistema di gestione whistleblowing adottato dalla Società, l'ODV riveste anche il ruolo di soggetto gestore della segnalazione - Whistleblowing Officer/WO - riportando, all'esito dell'iter espletato di valutazione della segnalazione così come definito dalle procedure, solo al CDA.



L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento dal CDA e potrà, a sua volta, chiedere di essere ascoltato in qualsiasi momento, al fine di riferire sul funzionamento del Modello o su situazioni specifiche.

Sono assolutamente vietate forme di ritorsione, comportamenti discriminatori o comunque pregiudizievoli, in via diretta o indiretta, verso l'OdV. L'azione dell'Organismo dovrà esser improntata sui principi di legalità, rispetto delle regole e collaborazione. Qualsiasi tipo di ostruzionismo teso ad ostacolare tali attività di verifica funzionali all'attuazione del Modello, sarà immediatamente oggetto di segnalazione nei confronti dell'Organo Amministrativo da parte dell'OdV.

#### 6.5 Durata in carica, decadenza e revoca

L'OdV resta in carica per 3 (tre) anni, alla scadenza dei quali è previsto il tacito rinnovo, garantendo, così, la continuità d'azione. Allo scadere dei 3 (tre) anni, qualora l'Organo Amministrativo non intenda rinnovare tacitamente l'incarico, dovrà notificare revoca formale all'OdV per iscritto.

Ricorre la decadenza dell'OdV quando vengono meno le condizioni di onorabilità e di indipendenza, nonché in caso di omessa vigilanza.

La revoca anticipata è prevista solo in presenza di gravi violazioni che integrino giusta causa, riscontrate nell'esecuzione dei propri doveri.

#### 6.6 Flussi informativi dell'ODV nei confronti del vertice societario

##### **Assetto organizzativo interno.**

All'ODV devono essere trasmessi e tenuti costantemente aggiornati i documenti afferenti al sistema di procure e deleghe in vigore presso la Società. In quanto parte integrante dell'assetto societario, l'ODV dovrà esser sempre messo al corrente delle variazioni organizzative e strutturali intraprese dal vertice societario il quale potrà interpellare tale organo sulla aderenza delle azioni intraprese ai principi del Decreto.

##### **Segnalazioni di esponenti aziendali o di terzi.**

Allo stesso tempo, dovrà essere portata a conoscenza dell'OdV qualunque informazione, di qualsiasi tipo, che sia giudicata attinente all'attuazione del Modello nelle aree di attività a rischio così come individuate nel Modello. L'obbligo riguarda principalmente le risultanze delle attività poste in essere dalla Società, nonché le atipicità e le anomalie riscontrate.

A tale riguardo valgono le seguenti prescrizioni:

- devono essere raccolte le segnalazioni relative a possibili ipotesi di commissione di reati previsti dal Decreto o, comunque, di condotte non in linea con le regole di condotta adottate dalla società;
- l'ODV valuterà le segnalazioni ricevute e adotterà i provvedimenti conseguenti, dopo aver ascoltato, se ritenuto opportuno, l'autore della segnalazione ed il responsabile della presunta violazione;
- le segnalazioni potranno essere effettuate in forma scritta ed avere ad oggetto ogni violazione o sospetto di violazione del Modello e delle procedure aziendali adottate. L'ODV agirà in modo da garantire i soggetti segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando, altresì, l'assoluta riservatezza dell'identità del segnalante;

Oltre a ciò, devono essere necessariamente trasmesse all'ODV tutte le informazioni che presentino elementi rilevanti in relazione all'attività di vigilanza, come ad esempio:

- i provvedimenti o le notizie provenienti da organi di polizia o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini per i reati di cui al Decreto;
- tutte le richieste di assistenza legale effettuate dalla Società;
- l'eventuale richiesta per la concessione di fondi pubblici in gestione o per l'ottenimento di forme di finanziamento dei fondi già in gestione;
- le notizie relative all'attuazione, a tutti i livelli aziendali, del Modello organizzativo con evidenza dei procedimenti disciplinari intrapresi e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti.

Relativamente agli obblighi di informativa valgono al riguardo le seguenti prescrizioni:

- l'afflusso di segnalazioni deve essere canalizzato verso l'OdV tramite un canale istituito *ad hoc* dall'azienda;
- l'OdV, valutate le segnalazioni ricevute, sentite le parti coinvolte (autore della segnalazione e presunto responsabile della violazione), determinerà i provvedimenti del caso;
- le segnalazioni dovranno essere formalizzate per iscritto;
- le stesse dovranno riguardare ogni violazione o sospetto di violazione del Modello.

Spetta all'OdV e al CDA il compito di garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante e la tutela dei diritti dell'azienda o delle persone accusate erroneamente e/o in mala fede.

## 6.7 Budget

Nel contesto delle procedure di formazione del budget, il Consiglio di Amministrazione, per garantire l'autonomia dell'OdV, dovrà approvare una dotazione adeguata di risorse finanziarie, eventualmente su proposta dall'Organismo stesso, della quale questo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti, tra i quali le consulenze specialistiche. Qualora si rendesse necessario l'espletamento di attività aggiuntive rispetto a quanto previsto nel piano annuale, l'OdV potrà richiedere la convocazione del Consiglio di Amministrazione per una revisione dei limiti di spesa.

L'OdV può avvalersi di risorse esterne per lo svolgimento delle seguenti attività:

- aggiornamento del processo di *risk assessment* 231 in particolare a seguito di mutamenti organizzativi o di business;
- aggiornamenti della normativa ed in particolare all'entrata in vigore di nuove fattispecie di reati;
- definizione e aggiornamento di protocolli e procedure in relazione a nuove fattispecie di reati;
- individuazione delle informazioni relative alle aree a rischio 231 rilevanti ai fini del monitoraggio attraverso i flussi informativi;
- consulenza su particolari temi specifici quali per esempio salute e sicurezza sui luoghi di lavoro, ambiente, privacy e sicurezza informatica;
- attività di supporto alle attività di verifica e corretta attuazione dei protocolli;
- attività di formazione e informazione.

## 7. Il progetto di adeguamento alla normativa intrapreso da Infodata S.p.A.

### 7.1 Obiettivi e finalità perseguiti con l'adozione del Modello 231

Infodata S.p.A. da sempre è sensibile all'esigenza di assicurare condizioni di correttezza e

trasparenza nella conduzione delle attività aziendali: infatti, a prescindere dal Modello, è stato avviato un Progetto di analisi dei propri strumenti organizzativi e di gestione volto a verificare la rispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto. Tale azione ha coinvolto anche le società controllate dalla stessa e, quindi, a livello di Gruppo, al fine di assicurare programmi di legalità condivisi, concreti nel rispetto delle singole individualità societarie.

È comune convinzione che l'adozione del Modello possa costituire un valido strumento di sensibilizzazione di tutti coloro che operano in nome e per conto della Società, affinché tengano comportamenti corretti e lineari nell'espletamento delle proprie attività, tali da prevenire il rischio di commissione dei reati previsti dal Decreto stesso.

In particolare, l'adozione del Modello consente di:

- determinare, in tutti coloro che operano nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, nella commissione di illeciti passibili di sanzioni penali comminabili nei loro stessi confronti e di sanzioni amministrative irrogabili ad Infodata S.p.A.;
- ribadire che tali forme di comportamento illecito sono fortemente condannate dalla Società, in quanto le stesse (anche nel caso in cui vi fosse apparentemente una condizione di vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche al Codice Etico e di Comportamento Infodata S.p.A.;
- consentire ad Infodata S.p.A., grazie ad un'azione di monitoraggio sulle aree di "Attività a rischio", di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

A tal fine, la Società ha predisposto una mappatura delle attività aziendali e, nell'ambito delle stesse, ha individuato le attività "a rischio" ovvero quelle che, per loro natura, rientrano tra le attività da sottoporre ad analisi e monitoraggio alla luce delle prescrizioni del Decreto.

E' impegno costante della Società svolgere un continuo monitoraggio della propria attività sia in relazione ai suddetti reati, sia in relazione all'espansione normativa cui potrà essere soggetto il Decreto 231: nel caso in cui dovesse emergere la rilevanza di uno o più dei reati sopra menzionati, o di eventuali nuovi reati inseriti nell'ambito del Decreto 231, la Società valuterà la necessità di integrare il presente Modello con nuove misure di controllo e/o nuove Parti Speciali.

## 7.2 Elementi fondamentali del Modello

I punti fondamentali individuati da Infodata S.p.A. nella definizione del Modello possono essere così, in sintesi, riassunti:

- valutazione del Sistema di Controllo Interno (SCI);
- coinvolgimento di tutti i soggetti che fanno parte della Società e che quotidianamente pongono in essere azioni rivolte al raggiungimento dello scopo sociale;
- segmentazione dei singoli ruoli e definizione delle responsabilità in base al ruolo rivestito all'interno di Infodata S.p.A. o delegate;
- mappatura delle attività aziendali "sensibili" ovvero di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto e pertanto da sottoporre ad analisi e monitoraggio;
- analisi dei protocolli in essere e definizione delle eventuali implementazioni finalizzate, con riferimento alle attività aziendali "sensibili", a garantire i principi di controllo;

- individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- recepimento delle procedure aziendali in essere e/o implementazione delle stesse in ottica di definizione di ulteriori presidi organizzativi strumentali all'attenuazione del rischio reato in astratto verificabile;
- riconoscimento dei rischi sottesi all'operatività quotidiana attraverso la predisposizione di un documento di valutazione *ad hoc*;
- definizione di un sistema disciplinare interno capace di sanzionare le condotte in violazione del MOG da parte dei Destinatari;
- Procedure di gestione delle segnalazioni Whistleblowing (PGSW);
- identificazione dell'OdV, ed attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- definizione dei flussi informativi nei confronti dell'Organismo;
- diffusione del MOG 231 nell'ambito di tutta la compagine societaria secondo canali che ne garantiscano il più ampio recepimento;
- attività di formazione, informazione, sensibilizzazione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- monitoraggio costante ed efficace da parte delle funzioni aziendali preposte con il supporto dell'OdV funzionale a testare l'idoneità del documento alla prevenzione dei reati presupposto successiva alla sua approvazione.

### 7.3 Modello, Codice Etico e Sistema disciplinare

Infodata S.p.A. ha ritenuto opportuno formalizzare i principi etici a cui quotidianamente si ispira nella gestione delle attività aziendali all'interno di un Codice Etico e di Comportamento, in considerazione anche delle condotte che possono determinare la commissione dei reati previsti dal Decreto.

Tale spirito è presente anche a livello di Gruppo: il Gruppo Infodata, infatti, si è dotato di un Codice Etico di Gruppo, condiviso e recepito dai vertici societari delle società controllate.

Grazie al Codice Etico, Infodata vuole perseguire i seguenti obiettivi:

- improntare su principi di correttezza, trasparenza e legalità i rapporti con soggetti terzi ed in particolar modo con la Pubblica Amministrazione;
- richiamare l'attenzione del personale dipendente, dei collaboratori, dei fornitori, e, in via generale, di tutti gli operatori, sul puntuale rispetto delle leggi vigenti, delle norme previste dal Codice etico, nonché delle procedure a presidio dei processi aziendali;
- richiamare i Destinatari il valore dei principi in esso sottesi, definendo un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

I principi di riferimento del Modello si integrano con quelli del Codice Etico adottato dalla Società e, in riferimento ai rapporti tra Modello e Codice Etico, è opportuno precisare che:

- il Codice Etico riveste una portata generale nonché contrattuale, in quanto contiene una serie di principi di "deontologia aziendale" che la Società riconosce come propri e sui quali intende richiamare l'osservanza di tutti i suoi dipendenti e di tutti coloro che cooperano al perseguimento dei fini aziendali;
- il Codice Etico rimanda al sistema disciplinare aziendale atto a sanzionare il mancato rispetto delle misure indicate nel Modello, previsto all'art.6, co.2 lett.e) del Decreto;

- il Modello risponde, invece, a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi nell'interesse o a vantaggio dell'azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

#### 7.4 Il ruolo delle Linee guida di Confindustria e l'applicazione delle norme nella costruzione del Modello

Per espressa previsione legislativa (art.6, co.3, d.lgs.231/01), i Modelli di organizzazione e di gestione possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia, il quale, di concerto con i Ministeri competenti, potrà formulare, entro 30 giorni, osservazioni sull'idoneità dei modelli a prevenire i reati.

La società si è ispirata alle "Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ai sensi del d.lgs. 231/01" elaborate da Confindustria nel 2002 e aggiornate nel marzo 2014.

Le Linee guida di Confindustria indicano un percorso che può essere in sintesi così riepilogato:

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

I punti cardine del sistema di controllo preventivo dei reati dolosi ideato da Confindustria sono:

- Codice Etico con riferimento ai reati considerati,
- sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro,
- procedure manuali e informatiche ("devono essere tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo"),
- poteri autorizzativi e di firma,
- comunicazione al personale e sua formazione,
- sistemi di controllo integrato.

Per quanto concerne, invece, i sistemi di controllo preventivo dei reati colposi in materia di tutela della salute e sicurezza sul lavoro e dell'ambiente, le Linee Guida, oltre a quanto già indicato per i reati dolosi, individuano la necessità di una particolare struttura organizzativa, adeguati livelli di formazione e addestramento, efficaci forme di circolazione e coinvolgimento degli interessati sul tema della salute e sicurezza sul lavoro ed un sistema di monitoraggio sistematico delle misure adottate.

Le Linee Guida, stabiliscono, altresì, una serie di "principi di controllo" a cui le componenti del sistema di controllo debbano ispirarsi:

- ogni operazione, transazione, azione deve essere verificabile, documentata, coerente e congrua;
- nessuno può gestire in autonomia un intero processo;
- i controlli devono essere documentati.

Il mancato rispetto di punti specifici delle predette Linee Guida non inficia la validità del Modello dal momento che il Modello adottato dall'ente deve essere necessariamente redatto con specifico riferimento alla realtà concreta della società, e pertanto lo stesso può anche discostarsi dalle Linee Guida di Confindustria, le quali, per loro natura, hanno carattere generale.

Nella costruzione del proprio MOG 231 poi, Infodata S.p.A. ha sfruttato l'adesione alle norme internazionali di riferimento che compongono il proprio SGI cui essa risulta costantemente

conferme.

#### 7.5 La costruzione del MOG di Infodata S.p.A.: il “Progetto 231”

Il “Progetto 231” intrapreso dalla Società al fine di dotarsi di un modello organizzativo idoneo a prevenire il verificarsi di uno dei reati presupposto previsti dal Decreto, si inserisce in un più ampio programma di organizzazione aziendale e di Gruppo, teso ad impostare una politica globale e condivisa di gestione aziendale consapevole e, soprattutto, in linea con i principi di etica d’impresa.

Al fine di divulgare comportamenti etici, improntati alla legalità, capaci, cioè, di allontanare i Destinatari dal porre in essere condotte poco trasparenti o divergenti da quanto definito preliminarmente a livello verticistico, la Società ha inteso trasmigrare nel proprio MOG la sua operatività quotidiana, in considerazione anche della sua propensione all’agire organizzato in ragione della pregressa e consolidata operatività interna che si conforma a norme e standard tecnici soggette a certificazione.

Il “Progetto 231” ha preso in considerazione l’intera realtà aziendale, tenendo in debita considerazione il ruolo della Società quale capogruppo del Gruppo Infodata, nonché del suo assetto organizzativo interno, che poggia la sua essenza sulla strutturazione di un Sistema di Gestione Integrato, ritenuto di fondamentale importanza per la gestione dei processi interni.

Le fasi del progetto hanno seguito il presente programma:

- valutazione preventiva del sistema normativo interno, ovvero esame dello statuto e della struttura organizzativa dell’Ente, delle procedure emanate per lo svolgimento dei processi operativi, del funzionigramma, degli ordini di servizi, nonché del sistema di procure e deleghe;
- analisi del contesto di riferimento attraverso la valutazione di quegli eventi pregiudizievoli rilevanti ai fini del d.lgs.231/01 che hanno coinvolto la Società;
- identificazione/aggiornamento dell’elenco delle possibili aree a “rischio reato”, intese come processi nei quali potrebbe astrattamente concretizzarsi la commissione dei reati presupposto. Nell’ambito di ciascuna delle suddette aree, sono poi state individuate/aggiornate le attività “sensibili”, ovvero quelle al cui espletamento è connesso il rischio di commissione dei reati previsti dal Decreto, nonché le funzioni aziendali potenzialmente esposte al rischio. Per ognuna delle aree a “rischio reato” si è quindi provveduto ad individuare quelle che possono essere considerate, in astratto e in via esemplificativa, le principali potenziali modalità di commissione dei reati presi in considerazione. L’esito di tali attività è stato rappresentato in un documento denominato MOG231\_INFORDATASPA\_RISKMAAPPING\_VER.1.0\_2021 (“Mappa delle aree e valutazione del rischio”);
- prendendo a riferimento la “Mappa delle aree a rischio”, rilevazione e analisi dei controlli esistenti idonei a prevenire il rischio di commissione dei reati. In particolare, l’analisi è stata condotta utilizzando la documentazione relativa alla Società, nonché attraverso un metodo di analisi (c.d. “*risk assessment*”) basato sullo svolgimento di colloqui con gli *owner* dei processi aziendali che, in ragione del ruolo ricoperto, risultano provvisti della più ampia e profonda conoscenza dell’operatività del settore aziendale di relativa competenza. Il coinvolgimento delle figure professionali aziendali ha consentito per ciascuna area, ove si è ritenuto potesse determinarsi il rischio di commissione dei reati, di effettuare la ricognizione delle modalità operative e gestionali esistenti e dei controlli aziendali presenti, a presidio delle stesse;



- sulla scorta di tali attività, individuazione degli ambiti di miglioramento dei controlli (c.d. “*gap analysis*”) e conseguente definizione del piano di rafforzamento del sistema di controllo interno rilevante ai fini del Decreto;
- valutazione del rischio attraverso la costruzione di una “metodologia per la valutazione della rischio inerente e residuale delle aree a “rischio reato” ex d.lgs.231/01 utilizzando un approccio in linea con le *best practice* di riferimento, le indicazioni fornite da Confindustria nell’ambito delle Linee Guida per la costruzione dei Modelli 231;
- definizione della PARTE SPECIALE, suddivisa in tante SEZIONI per le famiglie di reato presupposto che, in ragione degli esiti ottenuti dalle indagini effettuate, astrattamente potrebbero verificarsi nell’azione sociale da parte dei Destinatari. Tali sezioni definiscono, altresì, protocolli operativi e comportamentali che mirano a veicolare l’operatività interna verso condotte in linea con i dettami giuridici di riferimento, con efficacia dissuasiva per coloro i quali siano coinvolti nelle aree a rischio.

Attraverso la definizione di specifiche SEZIONI di PARTE SPECIALE, Infordata S.p.A. ha compiuto l’integrazione tra il SGI e il nuovo assetto organizzativo sviluppato con il MOGC 231, definendo, così, una concreta armonizzazione delle politiche operative di prevenzione del rischio reato; tale progetto ha, altresì, prodotto un’implementazione ulteriormente dei presidi preventivi in essere, concepiti ora come difensivi verso condotte trasgressive dell’organizzazione interna che potrebbero incidere sulla stabilità dell’intera compagine societaria.

### 8. Destinatari del Modello

Il Modello organizzativo è diffuso nell’ambito della struttura di Infordata S.p.A., secondo gli strumenti ritenuti dal vertice societario più idonei a garantire l’effettiva conoscenza dei principi nonché il recepimento dei contenuti.

Tutti coloro che operano in nome e per conto della Società per il conseguimento dello scopo e degli obiettivi sociali, sono da considerarsi quali destinatari, (di seguito, i “Destinatari”) del Modello.

Fra i Destinatari del Modello si possono annoverare:

- l’Organo Amministrativo, nel perseguimento dell’azione societaria in tutte le determinazioni adottate;
- i componenti dell’Organo di Controllo societario e Revisione contabile, nelle attività di controllo e nella verifica della correttezza formale e legittimità sostanziale dell’attività della Società e del funzionamento del sistema di controllo interno e della gestione dei rischi;
- tutti i dipendenti e tutti i collaboratori con cui si intrattengono rapporti contrattuali, a qualsiasi titolo, anche occasionali e/o soltanto temporanei;
- tutti coloro che intrattengono rapporti a titolo oneroso o anche gratuito di qualsiasi natura con la Società, c.d. “terze parti”.

**È fatto obbligo, pertanto, a tutti i Destinatari di aderire a quanto prescritto nel MOG 231 nonché a quanto previsto dai documenti in esso richiamati, in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici di natura giuslavoristica, commerciale e di ogni altra natura instaurati con Infordata S.p.A.**

**Il sistema disciplinare interno prevede specifiche sanzioni per coloro i quali non intendano uniformarsi ai principi nel MOG trascritti.**

### 9. Il sistema sanzionatorio 231 di Infordata S.p.A.

L'art.6, co.2, lett.e) e l'art.7, co.4, lett.b) del d.lgs.231/01 stabiliscono, con riferimento sia ai soggetti in posizione apicale che ai soggetti sottoposti ad altrui direzione, la necessaria predisposizione di *“un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello”*.

La previsione di un adeguato sistema che risulti idoneo a sanzionare le violazioni delle disposizioni e delle procedure organizzative richiamate dal Modello rappresenta un elemento qualificante dello stesso ed una condizione imprescindibile per la sua concreta operatività, applicazione e rispetto da parte di tutti i destinatari.

Al riguardo, è opportuno puntualizzare che l'applicazione delle sanzioni prescinde dalla concreta commissione di un reato e dall'eventuale instaurazione di un procedimento penale: la finalità delle sanzioni previste è infatti quella di reprimere qualsiasi violazione di disposizioni del Modello dettate ai fini della prevenzione di illeciti penali, promuovendo nel personale aziendale e in tutti coloro che collaborano a qualsiasi titolo con la Società, la consapevolezza della ferma volontà di quest'ultima di perseguire qualsiasi violazione delle regole poste a presidio del corretto svolgimento delle mansioni e/o degli incarichi assegnati.

Infodata S.p.A. si è dotata di un proprio sistema disciplinare 231, contrassegnato dal codice MOG231\_INFORDATASPA\_CODICEDISCIPLINARE231\_VER.1.0\_2021, cui si rimanda per le parti qui non regolamentate.

### 9.1 Violazione del Modello

A mero titolo esemplificativo, costituiscono violazione del Modello:

- la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello, ovvero l'omissione di azioni o comportamenti prescritti dal Modello, nell'espletamento di attività nel cui ambito ricorre il rischio di commissione dei reati (ossia nei c.d. processi sensibili) o di attività a questi connesse;
- la messa in atto di azioni o comportamenti non conformi ai principi contenuti nel Codice - Etico, ovvero l'omissione di azioni o comportamenti prescritti dal Codice Etico, nell'espletamento dei processi sensibili o di attività a questi connesse.

Con particolare riferimento alla normativa aziendale in materia di segnalazioni *whistleblowing*:

- la messa in atto di azioni o comportamenti in violazione delle misure poste a tutela del segnalante;
- l'adozione di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- l'effettuazione, in malafede o con grave negligenza, di segnalazioni che si rivelino infondate;
- violazioni delle Procedure di gestione delle segnalazioni Whistleblowing.

### 9.2 Misure nei confronti dell'Organo Amministrativo

La Società valuta con rigore le infrazioni al presente Modello poste in essere da coloro che rappresentano il vertice della Società e ne manifestano l'immagine verso i dipendenti, i soci, i creditori e il pubblico. La formazione e il consolidamento di un'etica aziendale sensibile ai valori della correttezza e della trasparenza presuppongono, anzitutto, che tali valori siano acquisiti e rispettati da coloro che guidano le scelte aziendali, in modo da costituire esempio e stimolo per tutti coloro che, a qualsiasi livello, operano per la Società.



### 9.3 Misure nei confronti dei Sindaci, Revisori e ODV

Stesso dicasi per gli organi di controllo previsti dalla legge, atti a vigilare sull'attività degli amministratori e controllare che la gestione e l'amministrazione della Società si svolgano nel rispetto della legge e dell'atto costitutivo.

### 9.4 Misure e sanzioni nei confronti dei dipendenti

L'inosservanza del Modello 231 adottato dalla Società ai sensi del Decreto, così come di ogni altro documento ad esso collegato o riferibile, implica l'apertura di una fase di accertamento del fatto e l'irrogazione di sanzioni disciplinari le quali, in ragione della categoria di Destinatari, troveranno la loro fonte nel rispetto delle procedure previste dall'art.7 della L.300/1970 ed eventuali norme speciali applicabili, le disposizioni del codice civile, i contratti.

### 9.5 Le misure e le sanzioni nei confronti dei soggetti aventi rapporti contrattuali con la società

L'inosservanza delle norme indicate nel Modello da parte di fornitori, collaboratori, consulenti esterni, *partner* aventi rapporti contrattuali/commerciali con l'azienda, può determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale e in ragione del fatto accertato, la risoluzione del relativo contratto, fermo restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte dell'Autorità Giudiziaria delle misure previste dal Decreto.

La Società si avvale di una specifica clausola, definita "CLAUSOLA 231", inserita nei contratti stipulati con terze parti, che obbligano quest'ultime ad adeguarsi ai principi sanciti nel proprio MOG 231.

## **10. Modifica, implementazione e verifica del funzionamento del Modello**

### 10.1 Modifiche ed integrazioni dei principi di riferimento del Modello

Il CDA provvede ad effettuare le successive ed eventuali modifiche e integrazioni dei principi di riferimento del Modello, allo scopo di consentire la continua rispondenza dello stesso alle prescrizioni del Decreto ed alle eventuali mutate condizioni della struttura dell'Ente.

Tale attività potrà esser delegata anche all'Amministratore Delegato che provvederà a presentare le modifiche all'attenzione del CDA.

### 10.2 Implementazione del Modello ed attuazione dei controlli sulle aree di attività a rischio

Il CDA provvede all'attuazione del Modello, mediante valutazione ed approvazione delle azioni necessarie per l'implementazione degli elementi fondamentali dello stesso; per l'individuazione di tali azioni, si avvale del supporto dell'Organismo di Vigilanza.

Il CDA deve altresì garantire, anche attraverso l'intervento dell'Organismo di Vigilanza, l'aggiornamento del Modello, in relazione alle esigenze che si rendessero necessarie nel futuro.

L'efficace e concreta attuazione del Modello deliberato ed approvato dal CDA è verificata dall'Organismo di Vigilanza, nell'esercizio dei poteri di controllo allo stesso conferiti sulle attività svolte dalle singole funzioni aziendali nelle aree a rischio.

Ogni modifica, integrazione e implementazione del MOG dovrà esser opportunamente tracciata, attraverso la compilazione della griglia di revisione di cui al frontespizio di ogni documento, avendo cura di modificarne la cronologia del codice, la data e la descrizione delle ragioni che

hanno condotto all'adozione della nuova versione.

### **11. Informazione, formazione ed aggiornamento**

Al fine di promuovere una cultura di impresa ispirata al rispetto della legalità e della trasparenza, Infodata S.p.A. assicura l'ampia divulgazione del Modello e l'effettiva conoscenza dello stesso da parte di chi è tenuto a rispettarlo.

In sede di prima adozione il MOG è messo a disposizione degli Organi sociali, dell'Organismo di Vigilanza, di ciascun dipendente e di ciascun soggetto tenuto a rispettare le prescrizioni del Modello.

Il Modello approvato dal CDA - nonché una copia di ogni intervenuta modifica e aggiornamento - è disponibile per la consultazione:

- presso la sede legale della Società;
- è inserito nel server aziendale, al fine di consentire ai Destinatari una consultazione giornaliera;
- pubblicato per estratto sul sito istituzionale della Società al fine di renderlo disponibile a tutte le parti interessate.

Prima dell'entrata in servizio ai dipendenti neo-assunti verrà messa a disposizione una copia del Modello e dovranno seguire i corsi di formazione dedicati, al fine di recepirne i contenuti in modo guidato.

L'adozione del Modello e le sue successive modifiche ed integrazioni, sono portate a conoscenza di tutti i soggetti con i quali l'azienda intrattiene rapporti d'affari rilevanti.

La Società predisponde, ogni anno, un piano di interventi formativi per i propri dipendenti e per le figure apicali al fine della completa acquisizione dei contenuti del modello di gestione. La partecipazione a tali eventi formativi è obbligatoria e seguirà le tempistiche e le modalità che di volta in volta Infodata S.p.A. riterrà più idonee ad esempio incontri, eventi formativi, lezioni frontali in aula, formazione dedicata suddivisa per aree di rischio o funzioni societarie, *e-learning*. La mancata partecipazione a tali incontri formativi sul MOG231 costituirà fonte di illecito disciplinare.

I contenuti degli incontri formativi potranno esser concordati dall'Organo amministrativo con l'Organismo di Vigilanza, il quale potrà esprimere una valutazione non vincolante e/o suggerire modifiche ai piani proposti.