

**MODELLO DI ORGANIZZAZIONE, GESTIONE E  
CONTROLLO  
AI SENSI DEL D.LGS. 231/01**



## Sommario

1.	Profilo della società	3
2.	Normativa	3
3.	Elemento fondanti e presupposti d'esclusione della responsabilità dell'Ente	5
4.	Struttura del Modello CIO	5
5.	Destinatari del modello	6
6.	Principi ispiratori ed elementi costitutivi del Modello	7
7.	Funzioni del Modello	7
8.	Modalità di costruzione del Modello	8
9.	Adozione del Modello	10
10.	Composizione dell'Organismo di Vigilanza	11
11.	Sistema disciplinare	12
12.	Formazione e diffusione del Modello Organizzativo	14

## 1. Profilo della Società

C.I.O. – Consorzio Interregionale Ortofrutticoli Società Cooperativa a responsabilità limitata (d’ora innanzi “CIO”) ha sede in Parma e rappresenta la più importante Associazione di Organizzazioni Produttori (AOP) di pomodoro da industria in Europa.

La condizione soggettiva di AOP le è stata riconosciuta nel 2003 dalla Regione Emilia-Romagna e confermata nel 2023 per i seguenti prodotti: pomodori (freschi o refrigerati), cipolle e scalogni, aglio, cavolfiori e cavoli broccoli, cavoli bianchi e cavoli rossi, altri ortaggi e legumi, cocomeri, meloni, piselli, fagioli.

A costituire la sua base associativa sono le Organizzazioni di Produttori AINPO, Consorzio Casalasco del Pomodoro e P.O.A, che associano oltre 800 soci in grado di produrre ogni anno oltre 1 milione di tonnellate di pomodori freschi, coltivando terreni estesi per oltre 14.000 ettari, che costituiscono circa il 36% delle superfici coltivate a pomodoro destinato alla trasformazione nel nord Italia.

La principale funzione dell’AOP CIO è costituita dall’offerta di servizi a supporto dei soci, che vanno dall’acquisizione del seme (interpretando, di fatto, un ruolo di “centrale d’acquisto” per i soci stessi), ai controlli sull’intera filiera fin dalle prime fasi di acquisto dello stesso e della produzione delle piantine per il trapianto del pomodoro in campo, alla coltivazione e trasformazione attraverso sperimentazioni, analisi e verifiche qualitative.

Come AOP a CIO compete lo sviluppo dei Programmi Operativi, che rappresentano la strategia elaborata dall’AOP per raggiungere gli obiettivi prefissati dalle norme comunitarie e nazionali.

I programmi operativi sono attuati attraverso interventi sviluppati nelle singole annualità.

CIO elabora un proprio programma operativo a cui tutte le OO.PP. socie possono partecipare, ne gestisce gli aspetti finanziari e lo rendiconta.

Le attività pianificate nel programma operativo trovano il loro supporto economico-finanziario nel Fondo di esercizio, nel quale confluiscono le risorse finanziarie comunitarie e degli associati a supporto degli interventi previsti ed approvati dalle competenti Autorità (Regione).

Nella sua essenza CIO coordina e gestisce, svolgendo un’attività sottoposta ad una stringente regolamentazione, le risorse finanziarie in parte di provenienza comunitaria che servono per attuare gli interventi previsti nei programmi operativi.

Di qui la specificità che ha caratterizzato l’analisi dei rischi alla base del presente modello, laddove, in assenza delle classiche criticità che s’associano a contesti logistico-produttivi (sicurezza sul lavoro, temi ambientali), ad organigrammi con complesse articolazioni funzionali (qui, di converso, assai semplificati e fondati sulla strutturazione binaria in macroaree amministrativa ed agronomica), se ne profilano d’altra natura, suscitate dalla prossimità con le Pubbliche Amministrazioni.

## 2. Normativa

Il Decreto Legislativo 231/2001 e le sue successive modifiche ed integrazioni, recante le disposizioni normative concernenti la “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” (di seguito “Decreto”), ha introdotto nell’ordinamento italiano la responsabilità della persona giuridica qualora determinati reati siano stati commessi nel suo interesse o a suo vantaggio:

- a) da persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (Soggetti Apicali), nonché da persone fisiche che esercitano, anche di fatto, la gestione e il controllo della stessa;
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati alla precedente lettera a) (ad esempio, dipendenti).

Si sottolinea che la responsabilità della società è:

- “aggiuntiva e non sostitutiva” a quella delle persone fisiche che hanno realizzato materialmente il reato (responsabilità che quindi resta regolata dal diritto penale comune);
- diretta ed autonoma rispetto a quella della persona fisica.

La responsabilità amministrativa introdotta dal Decreto mira innanzitutto a colpire il patrimonio degli enti che abbiano tratto un vantaggio dalla commissione di alcune, individuate, fattispecie criminose (reati – presupposto).

Per tali motivi l'apparato sanzionatorio predisposto dal legislatore in caso di commissione dei Reati ha il preciso intento di colpire direttamente ed in modo efficace la persona giuridica con la previsione di quattro differenti tipi di sanzione, che si prescrivono nel termine di cinque anni dalla data di consumazione del reato (art. 22): le sanzioni amministrative pecuniarie (art.10), le sanzioni interdittive (art.13), la pubblicazione della sentenza (art. 18) e la confisca (art.19).

La sanzione base comminata per ogni illecito amministrativo dipendente da Reato, che costituisce il perno del sistema sanzionatorio del decreto, è la sanzione pecuniaria.

Nella commisurazione della suddetta sanzione si fa riferimento ad un duplice limite quantitativo e qualitativo attraverso il sistema delle quote: in relazione a ciascun Reato viene stabilita una quota, che deve necessariamente rispettare un quantum minimo e massimo, che si assesta tra le 100 e le 1000 quote e che può avere un valore che oscilla dai 258 euro ai 1.549 euro.

I criteri di riferimento per la determinazione del numero delle quote da irrogare (art.11 del Decreto) sono la gravità del fatto, il grado di responsabilità dell'ente e l'attività messa in opera da quest'ultimo per prevenire il Reato.

Per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive temporanee (di durata non inferiore a 3 mesi e non superiore a 2 anni), quali:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o revoca di autorizzazioni o licenze o connessioni funzionali alla commissione dell'illecito;
- c) il divieto di contrattare con la Pubblica Amministrazione;
- d) l'esclusione da finanziamenti agevolati o simili sussidi, o revoca di quelli già concessi;
- e) il divieto di pubblicizzazione dei beni o servizi.

Il giudice può erogare le predette misure quando ricorre almeno una delle seguenti condizioni:

- l'ente ha tratto dal Reato un profitto di rilevante entità ed il Reato è stato commesso da un soggetto in posizione apicale o da un soggetto sottoposto all'altrui direzione (in quest'ultimo caso, le carenze organizzative devono averne determinato o agevolato la commissione);
- sussiste la reiterazione dell'illecito.

Nei casi di applicazione delle sanzioni interdittive, può essere anche disposta la pubblicazione della sentenza di condanna.

### 3. Elementi fondanti e presupposti d'esclusione della responsabilità dell'Ente

Elemento costitutivo della responsabilità dell'ente è rappresentato dalla necessità che la condotta illecita ipotizzata sia stata realizzata “nell'interesse o a vantaggio della società” e non “nell'interesse esclusivo proprio o di terzi”.

Secondo la Relazione Ministeriale di accompagnamento al Decreto, la nozione di “interesse” ha fondamento soggettivo, indicando il fine in vista del quale il soggetto ha commesso il reato, mentre il “vantaggio” fa riferimento all'oggettiva acquisizione di un profitto da parte dell'ente.

Quanto ai criteri soggettivi di imputazione della responsabilità all'ente per il fatto di reato, va da sé che la responsabilità della persona giuridica viene ricollegata ad un difetto di organizzazione, consistente nel non avere posto in essere un piano di organizzazione, gestione e controllo idoneo a prevenire la commissione dei Reati.

Il Decreto prevede infatti, agli articoli 6 e 7, una forma di esonero dalla responsabilità per l'ente quando questo dimostri:

- di aver adottato ed efficacemente attuato un “Modello di Organizzazione, Gestione e Controllo” idoneo a prevenire la realizzazione dei Reati;
- di aver istituito un Organismo di Vigilanza all'interno della società, dotato di completa autonomia di iniziativa e controllo, nonché con specifici obblighi di vigilanza sul funzionamento, sull'osservanza del Modello e sul suo aggiornamento;
- che le persone che hanno commesso il Reato abbiano agito eludendo fraudolentemente il Modello;
- che non vi siano state omissioni o insufficiente vigilanza da parte dell'Organismo di Vigilanza preposto.

In particolare, per evitare la responsabilità, la società deve dimostrare l'assenza di colpa organizzativa, cioè che il Reato è stato commesso nonostante essa avesse adottato tutte le misure idonee alla prevenzione dei reati ed alla riduzione del rischio di loro commissione.

Resta inteso che il Modello per avere efficacia esimente deve rispondere alle seguenti esigenze:

- individuare le aree di rischio di commissione dei Reati attraverso un adeguato processo di valutazione dei rischi;
- predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a prevenire la commissione dei Reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- configurare un sistema disciplinare sanzionatorio per la violazione delle norme del codice etico, nonché delle procedure previste dal Modello stesso.

L'adozione del Modello è responsabilità dell'organo amministrativo.

Il Decreto prevede che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria.

### 4. Struttura del modello CIO

Il modello si compone delle seguenti parti:

- la presente **Parte Generale** ove sono illustrati il profilo della società, la normativa di riferimento, i principi ispiratori e gli elementi costitutivi del modello (sistema di corporate governance, sistema di controllo interno, principi del sistema deleghe, codice etico), la funzione del Modello, le modalità di costruzione del Modello, la sua struttura, i destinatari, i rapporti con i terzi, nonché il sistema disciplinare e le misure da adottare per la relativa formazione, diffusione e per le modifiche e l'aggiornamento;

- l'**elenco dei Reati 231**, di cui allegato B;

- il **codice Etico**, di cui all'allegato C, contenente il richiamo alla procedura "Whistleblowing" (all. D)

- Il modello si compone altresì dei "**Flussi informativi (verso l'Organismo di Vigilanza)**" elaborato che riepiloga in modo sintetico tutti i documenti e le informazioni che ogni area funzionale è chiamata a predisporre e fornire all'Organismo di Vigilanza al fine di assicurare la corretta e tempestiva informazione sui fondamentali aspetti della gestione, nonché del "**Regolamento dell'Organismo di Vigilanza**", di cui si è dotato l'Organismo di Vigilanza per svolgere le sue funzioni.

- le **Parti Speciali** e le relative Schede "Analisi Attività Sensibile" (ad uso esclusivo interno alla Società) nelle quali i reati presupposto sono raggruppati per aree tematiche, analizzati e selezionati se la loro commissione è ritenuta astrattamente ipotizzabile in ragione del profilo e dell'attività svolta in CIO; sono di seguito elencate:

- ❖ PARTE SPECIALE "A" – Igiene e Sicurezza sui luoghi di lavoro
- ❖ PARTE SPECIALE "B" – Reati Ambientali
- ❖ PARTE SPECIALE "C" - Reati Societari e di *Market Abuse*, Gestione Finanziaria
- ❖ PARTE SPECIALE "D" – Reati tributari e Doganali
- ❖ PARTE SPECIALE "E" – Rapporti con la Pubblica Amministrazione
- ❖ PARTE SPECIALE "F" - Reati Informatici, Trattamento Illecito di Dati, Violazione Proprietà Industriale e del Diritto di Autore, Falsità di Monete, Carte di Pubblico Credito, Valori di Bollo o segni di riconoscimento
- ❖ PARTE SPECIALE "G" – Altri Reati

Al termine della disamina di ogni Parte speciale, è stato descritto ed esplicitato il contenuto dei citati "Flussi" a beneficio dell'ODV.

## 5. Destinatari del presente modello

Le regole contenute nel Modello si applicano a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società, ai dipendenti, nonché a coloro i quali, pur non appartenendo alla Società direttamente, operano su mandato o sono legati a CIO da contratti rientranti nella c.d. para subordinazione.

La Società comunica il presente Modello attraverso le modalità più idonee per l'effettiva conoscenza da parte di tutti i soggetti interessati, i quali devono rispettare puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con CIO e a tal fine organizza attività formative volte a far conoscere il Modello a tutti i soggetti interessati.

CIO condanna qualsiasi comportamento che sia difforme alla legge e alle previsioni del Modello e del Codice Etico, anche qualora il comportamento sia realizzato nell'interesse di CIO ovvero con l'intenzione di arrecarle vantaggio.

## 6. Principi ispiratori ed elementi costitutivi del modello

La predisposizione, così come le successive attività di aggiornamento del Modello, hanno costituito un'occasione per rafforzare il Sistema di Controllo Interno e Gestione dei Rischi di CIO e sensibilizzare le risorse impiegate nel processo di elaborazione e di *risk assessment* rispetto al tema del controllo dei processi aziendali anche in un'ottica di prevenzione attiva dei Reati.

Nella predisposizione del proprio Modello, CIO si è ispirata alle "Linee Guida per la costruzione dei modelli di Organizzazione, Gestione e Controllo", elaborate da Confindustria. Il percorso da queste indicato per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

- individuazione delle aree a rischio, volta a verificare in quali aree/settori aziendali sia possibile la realizzazione dei reati;
- valutazione del sistema di controllo interno già implementato dalla società e individuazione delle eventuali aree di miglioramento nell'ottico di prevenzione dei Reati;
- predisposizione/aggiornamento del sistema di controllo al fine di ridurre i rischi attraverso l'adozione di appositi protocolli.

Al raggiungimento di tali obiettivi concorre l'insieme coordinato di tutte le strutture organizzative, attività e regole operative applicate – su indicazione del vertice apicale – dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno. Le componenti più rilevanti del sistema di controllo preventivo proposto da Confindustria sono:

- codice etico;
- sistema organizzativo;
- procedure manuali ed informatiche;
- poteri autorizzativi, procure e deleghe;
- sistemi di controllo e gestione;
- comunicazioni al personale e sua formazione.

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

- verificabilità, attitudine a documentare, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli.

## 7. Funzione del modello

Con l'adozione del Modello, CIO intende:

1. adempiere compiutamente alle previsioni di legge ed ai principi ispiratori del Decreto attraverso la formalizzazione di un sistema strutturato ed organico, già esistente in azienda, di procedure ed attività di controllo (preventivo ed *ex post*) volto a prevenire e presidiare il rischio di commissione dei Reati mediante l'individuazione delle relative Attività Sensibili;

2. costituire uno strumento efficace di gestione aziendale, riconoscendo al Modello anche una funzione di creazione e protezione del valore dell'azienda stessa.

Infatti, attraverso l'adozione del Modello, CIO si propone di:

- a) consolidare una cultura della prevenzione del rischio e del controllo nell'ambito del raggiungimento degli obiettivi aziendali;
- b) prevedere un sistema di monitoraggio costante dell'attività aziendale volto a consentire a CIO di reagire tempestivamente nel prevenire o impedire la commissione dei Reati stessi;
- c) fornire adeguata informazione ai dipendenti ed a coloro che agiscono su mandato o sono legati alla Società, in merito a:
  - (i) le attività che comportano il rischio di commissione dei Reati in caso di comportamenti non conformi alle prescrizioni del Codice Etico ed alle altre regole di condotta/procedure aziendali (oltre che alla legge);
  - (ii) le conseguenze sanzionatorie che possono derivare ad essi o alla Società per effetto della violazione di norme di legge o di disposizioni interne della Società.
- d) diffondere ed affermare una cultura d'impresa improntata alla legalità, con l'espressa riprovazione da parte di CIO di ogni comportamento contrario alla legge o alle disposizioni interne e, in particolare, alle disposizioni contenute nel presente Modello;
- e) prevedere un'efficiente ed equilibrata organizzazione dell'impresa, con particolare riguardo ai processi di formazione delle decisioni ed alla loro trasparenza, ai controlli, preventivi e successivi, nonché all'informazione interna ed esterna.

A tal fine, il Modello prevede misure idonee a migliorare l'efficienza nello svolgimento delle attività nel costante rispetto della legge e delle regole, individuando misure dirette ad eliminare tempestivamente situazioni di rischio.

In particolare, CIO adotta e attua scelte organizzative e procedurali efficaci per:

- a) assicurare che le risorse umane siano assunte, dirette e formate secondo i criteri espressi nel Codice Etico di CIO e in conformità alle norme di legge in materia, in particolare all'art. 8 dello Statuto dei Lavoratori;
- b) favorire la collaborazione alla più efficiente realizzazione del Modello da parte di tutti i soggetti che operano nell'ambito dell'impresa o con essa, anche garantendo la tutela e la riservatezza circa l'identità di coloro che forniscono informazioni veritiere e utili ad identificare comportamenti difforni da quelli prescritti;
- c) garantire che la ripartizione di poteri, competenze e responsabilità e la loro attribuzione all'interno dell'organizzazione aziendale siano conformi a principi di trasparenza, chiarezza, verificabilità e siano sempre coerenti con l'attività in concreto svolta dalla Società;
- d) prevedere che la determinazione degli obiettivi aziendali, a qualunque livello, risponda a criteri realistici e di obiettiva realizzabilità;
- e) individuare e descrivere le attività svolte dalla Società, la sua articolazione funzionale e l'organigramma aziendale in documenti costantemente aggiornati, con la puntuale indicazione di poteri, competenze e responsabilità attribuiti ai diversi soggetti, in riferimento allo svolgimento delle singole attività;
- f) attuare programmi di formazione, con lo scopo di garantire l'effettiva conoscenza del Codice Etico e del Modello da parte di tutti coloro che operano nell'impresa o con essa, che siano direttamente o indirettamente coinvolti nelle attività e nelle operazioni a rischio.

## **8. Modalità di costruzione del modello**

Al fine di garantire la predisposizione ed il costante aggiornamento del Modello ai sensi dell'art. 6 del Decreto, CIO ha intrapreso un processo di analisi del contesto aziendale volto ad evidenziare l'area



o il settore e con quali modalità si possano verificare i Reati di cui al Decreto, ispirandosi all'approccio metodologico di Confindustria, le cui principali fasi metodologiche sono di seguito descritte:

a) mettere in atto un **processo di valutazione dei rischi** composto delle seguenti due fasi:

- 1. Identificazione dei rischi:** *che si concretizza in un'analisi del contesto aziendale tale da evidenziare in quale area/settore di attività e secondo quali modalità si possano commettere i reati di cui al D. Lgs. 231/01.*
- 2. Progettazione del sistema di controllo:** *ossia la valutazione del sistema esistente all'interno dell'ente ed il suo eventuale adeguamento in termini di capacità di contrastare efficacemente, ossia ridurre ad un livello accettabile, i rischi identificati;*

b) prevedere un adeguato **sistema sanzionatorio** per la violazione delle norme del codice etico, nonché delle procedure previste dal Modello stesso. Simili violazioni ledono, infatti, il rapporto di fiducia instaurato con l'ente e devono di conseguenza comportare azioni disciplinari, a prescindere dall'eventuale instaurazione di un giudizio penale nei casi in cui il comportamento costituisca reato;

c) costituire un organismo dotato di autonomi poteri di iniziativa e controllo (di seguito "**Organismo di Vigilanza**") che possieda requisiti di autonomia, indipendenza, professionalità e onorabilità, e la competenza per vigilare sull'**effettività** del modello, per svolgere attività di disamina continuativa in merito all'**adeguatezza** dello stesso. In quest'ottica, CIO ha avviato una serie di attività, suddivise in diverse fasi, dirette alla costruzione di un sistema di prevenzione e gestione dei rischi in conformità al Decreto, che vengono di seguito espone:

Per l'analisi dei rischi potenziali CIO ha adottato il Modello con i reati inclusi nel D. Lgs. 231/01 sulla base di una analisi delle proprie attività sensibili, intervistando le preminenti figure aziendali, quelle coinvolte nelle funzioni di indirizzo, guida e controllo, con lo scopo di validare il grado di applicabilità in astratto delle fattispecie di Reato previste dal Decreto alla luce del Profilo della Società e degli specifici ambiti in cui CIO opera.

Ogniqualevolta la normativa 231 viene estesa a nuovi reati o mutano le condizioni di rischio nell'ambito dello svolgimento delle attività aziendali (e.g. apertura di nuove funzioni di *business*, cambiamenti dell'organizzazione, ecc.), ODV s'impegna a coinvolgere le funzioni interessate con lo stesso approccio metodologico qui di seguito meglio descritto al fine di effettuare l'aggiornamento.

Se si rendesse necessario procedere a un aggiornamento della mappatura delle attività/aree a rischio/sensibili e analisi dei relativi Protocolli di Controllo, ODV:

- identifica i temi di *compliance* rilevanti per il (nuovo o meno) *business*;
- esamina la normativa applicabile al citato *business* in relazione al quale viene condotta l'attività di *risk assessment* attraverso la mappatura delle leggi, della regolamentazione e delle *best practices* applicabili;
- definisce un *action plan* per l'attività di mappatura;
- identifica, in base alla natura del reato/attività sensibile, il possibile personale interno da coinvolgere eventualmente per l'analisi più approfondita dei reati astrattamente applicabili alla Società.

ODV deve procedere dunque a:

- identificare e analizzare le attività aziendali sensibili alla luce dei reati-presupposto;
- identificare i soggetti coinvolti nell'attività sensibile e le potenziali modalità attuative degli illeciti nelle aree a rischio individuate;
- identificare e valutare il sistema di controlli preventivi esistenti nelle attività sensibili, considerando l'ambiente di controllo aziendale e gli specifici protocolli di controllo;
- valutare il rischio residuo, predisponendo eventuali piani operativi di miglioramento;

- porre in essere un monitoraggio costante delle attività aziendali sensibili riferite alla propria direzione, attraverso la periodica revisione delle Schede Attività Sensibili, con il fine, tra l'altro, di mantenere costantemente aggiornata la mappatura delle attività/aree a rischio/sensibili e valutare l'idoneità e l'efficacia relativi Protocolli di Controllo adottati;

contribuendo così alla progettazione e al miglioramento continuo del Sistema di Controllo Interno e Gestione dei Rischi e all'informazione operativa per quanto di competenza.

Infine, l'Organismo di Vigilanza ha in ogni caso il potere/dovere di raccomandare ulteriori attività di miglioramento e richiedere l'analisi di ulteriori attività potenzialmente a rischio che, in funzione dell'evoluzione legislativa o dell'attività di CIO, potranno essere ricomprese nel novero delle Attività sensibili.

Nelle Parti Speciali del Modello sono riportati nel dettaglio l'identificazione delle attività sensibili, i soggetti coinvolti in tali attività ed i relativi protocolli di controllo attuati.

Sarà compito dell'OdV mettere in atto le raccomandazioni individuate in sede di mappatura dei rischi e verificare costantemente la congruità del modello, richiedendone i necessari adeguamenti sia rispetto a variazioni dell'assetto societario, sia rispetto ad eventuali variazioni normative.

Le raccomandazioni individuate comportano la necessità di sviluppare un piano di intervento volto alla:

- definizione dei processi aziendali con particolare riferimento ai livelli di responsabilità con il perfezionamento della separazione delle funzioni;
- definizione e verifica costante del piano di deleghe;
- costante e puntuale applicazione del Decreto Legislativo n° 81/2008 (Testo unico per la sicurezza sul lavoro);
- definizione, aggiornamento e informazione sulle procedure e *job description* aziendali.

## **9. Adozione del modello**

Conclusa l'attività di mappatura delle attività/aree a rischio/sensibili e analisi dei relativi Protocolli di Controllo (se presenti), in ossequio a quanto previsto dal D. Lgs. 231/2001 e dalle disposizioni codicistiche in tema di governo societario (in particolare, art. 2381 c.c.) il Consiglio d'Amministrazione di CIO delibera l'adozione (o l'aggiornamento) del Modello.

1. In aggiunta ai casi sopra citati (l'estensione della normativa 231 a nuovi reati o il mutamento delle condizioni di rischio nell'ambito dello svolgimento delle attività aziendali), il Consiglio di Amministrazione di propria iniziativa o su segnalazione dell'Organismo di Vigilanza provvede ad adeguare e aggiornare tempestivamente il Modello qualora siano individuate violazioni o elusioni delle prescrizioni in esso contenute che ne evidenziano l'inadeguatezza a garantire l'efficace prevenzione dei fatti di reato.
2. Le proposte di modifica del Modello devono essere preventivamente comunicate all'Organismo di Vigilanza, il quale deve esprimere un parere.
3. In deroga a quanto disposto dal punto precedente, il Presidente può apportare al Modello modifiche di natura non sostanziale, qualora necessarie per una sua miglior chiarezza od efficienza nonché adeguamenti puramente formali quali ad esempio l'aggiornamento della lista dei reati e l'elenco delle parti speciali nella parte generale del Modello, l'aggiornamento della descrizione di CIO etc. Di tali modifiche è data comunicazione al Consiglio di Amministrazione e all'Organismo di Vigilanza.
4. L'Organismo di Vigilanza, in ogni caso, deve prontamente segnalare in forma scritta, senza dilazione, al Presidente eventuali fatti che evidenziano la necessità di revisione del Modello. Il Presidente, in tal caso, deve convocare il Consiglio d'Amministrazione, affinché adotti le deliberazioni di sua competenza. Quanto previsto si applica, in quanto compatibile, per le modifiche delle procedure necessarie per l'attuazione del Modello, ad opera delle funzioni

interessate. Le modifiche alle procedure devono essere tempestivamente comunicate all'Organismo di Vigilanza, il quale deve esprimere il proprio parere.

5. Nell'eventualità in cui si rendesse necessario procedere all'emanazione di ulteriori Parti Speciali, relativamente a nuove fattispecie di reato che venissero in futuro ricomprese nell'ambito di applicazione del Decreto 231/01, è demandato al Consiglio d'Amministrazione, anche su proposta dell'Organismo di Vigilanza, il potere di integrare il presente Modello in una fase successiva, mediante apposita delibera.

## **10. Composizione dell'Organismo di Vigilanza**

L'OdV è nominato dal Consiglio d'Amministrazione, sentito il parere dell'Organo di Controllo, con una composizione (monocratica o collegiale) ed un mandato temporale definiti dall'Organo di Amministrazione stesso; deve essere dotato dei requisiti di seguito indicati:

### **Autonomia**

Ai sensi dell'art. 6 comma 1 lettera b) del Decreto, l'Organismo deve essere dotato di "autonomi poteri di iniziativa e controllo". I requisiti di autonomia e indipendenza presuppongono che l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo.

Si tratta di un'autonomia di tipo decisionale, inerente all'aspetto funzionale e qualificabile come imprescindibile libertà di autodeterminazione e d'azione, con pieno esercizio della discrezionalità tecnica nell'espletamento delle funzioni di un organismo autoreferenziale.

L'autonomia è in primo luogo rispetto alla società, ai suoi vertici ed al management; conseguentemente l'OdV deve poter espletare le sue funzioni completamente libero da condizionamenti o pressioni e non deve essere coinvolto nell'esercizio di attività di gestione che esorbitino dai compiti specificamente assegnati in funzione dell'attività sua propria.

Esso agisce in piena autonomia disponendo di mezzi finanziari adeguati ad assicurare la sua piena ed indipendente operatività. A tal fine, il Consiglio di Amministrazione attribuisce all'ODV, sulla base delle indicazioni del medesimo, una dotazione per le spese da sostenere nell'esercizio delle proprie funzioni, di cui l'ODV fornisce annualmente adeguata rendicontazione.

### **Professionalità**

L'Organismo di Vigilanza deve essere professionalmente capace ed affidabile, requisiti questi che debbono essere tipici dell'organo nel suo complesso e conseguentemente anche dei singoli membri che lo compongono. Deve disporre di tutte le cognizioni tecniche per espletare con la massima serietà ed efficacia le funzioni ad esso affidate (anche avvalendosi di competenze tecniche esterne, come previsto nel Regolamento dell'Organismo di Vigilanza, di seguito riportato). Tali caratteristiche unite all'indipendenza garantiscono l'obiettività di giudizio.

### **Continuità di azione**

Al fine di assicurare la garanzia di efficacia e costante attuazione del Modello è necessaria una struttura che lavori a tempo pieno alla vigilanza, al controllo ed al monitoraggio del rispetto e dell'adeguatezza del Modello, ossia capacità di esercitare in modo continuativo i poteri di controllo, al fine di assicurare una costante attività di monitoraggio e di analisi del sistema di prevenzione interno, disponendo dei necessari poteri d'indagine.

L'Organismo di Vigilanza nell'esecuzione delle proprie attività di controllo ha libero accesso a tutti i dati dell'azienda e può disporre di tutte le funzioni e strutture aziendali.

Riporta l'esito delle proprie verifiche anche al Collegio Sindacale.

### **Indipendenza**

Per indipendenza s'intende l'assenza di cause di ineleggibilità e decadenza di cui all'art. 2382 del cc. nonché l'assenza di vincoli di parentela e/o affinità entro il quarto grado con gli amministratori della società, o delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo. Sono altresì considerati indipendenti gli amministratori della società che sono in possesso dei requisiti di indipendenza ai sensi dell'Art 147 ter del TUF nonché di quelli di indipendenza ai sensi del Manuale di Corporate Governance.

### **Onorabilità**

Per onorabilità s'intende:

- (i) non essere stato sottoposto a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della Legge 27 dicembre 1956, n. 1423, o dalla Legge 31 maggio 1965, n. 575, e successive modifiche ed integrazioni, salvo gli effetti della riabilitazione;
- (ii) non essere stato condannato con sentenza irrevocabile, salvi gli effetti della riabilitazione:
  - a pena detentiva per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria e assicurata e dalle norme in materia di mercati e strumenti finanziari, in materia tributaria e di strumenti di pagamento;
  - alla reclusione, per uno dei delitti previsti nel titolo XI del libro V del codice civile e nel regio decreto del 16 marzo 1942, n. 267;
  - alla reclusione, per un tempo non inferiore a sei mesi per un delitto contro la pubblica amministrazione, la fede pubblica, il patrimonio, l'ordine pubblico e l'economia pubblica;
  - alla reclusione, per un tempo non inferiore ad un anno, per un qualunque delitto non colposo;
  - per le fattispecie di reato previste dal Decreto.
- (iii) non aver subito l'applicazione, su richiesta delle parti, di una delle pene previste al precedente punto 2, fatto salvo il caso dell'estinzione del reato.

### **Obbligo di informazione all'Organismo di Vigilanza**

Al fine di agevolare l'attività di vigilanza sul funzionamento ed efficacia, sull'osservanza e sull'aggiornamento del Modello nelle Attività sensibili, deve essere portata a conoscenza dell'ODV qualsiasi informazione, proveniente anche da terzi, attinente all'attuazione del Modello stesso. Le informazioni riguardano in genere tutte le notizie relative alla commissione dei reati previsti dal Decreto e dalle leggi successive, o a comportamenti non in linea con le regole di condotta adottate.

Tale obbligo di informazione all'ODV è rivolto:

- al management e alle funzioni aziendali di primo livello e alla struttura di Audit relativamente alle attività svolte nelle Aree Sensibili e riguarda:
  - 1. le risultanze periodiche dell'attività di controllo dalle stesse poste in essere per dare attuazione al Modello (informativa costante e periodica);
  - 2. le anomalie o atipicità riscontrare, all'occorrenza, nell'ambito delle informazioni disponibili (informazioni ad hoc);
- al personale di CIO ed ai suoi collaboratori, i quali hanno facoltà di rivolgersi direttamente all'Organismo di Vigilanza per segnalare irregolarità o violazioni del Modello stesso e del Codice Etico tramite l'apposito canale di segnalazioni (cfr. 4.11).

Le suddette informazioni e la documentazione da trasmettere e/o da mettere a disposizione dell'OdV, con le relative tempistiche ed i canali informativi da utilizzare, sono individuate nelle diverse linee guida, procedure ed istruzioni emesse dalla Società.

L'Organismo di Vigilanza di CIO si dota di un apposito regolamento che forma parte integrante del presente Modello.

## **11. Sistema Disciplinare**

Il Modello impone regole di condotta atte a prevenire la commissione dei reati di cui al Decreto e, più in generale, ad assicurare la corretta applicazione delle procedure interne previste (cfr. art. 6, comma secondo, lett. e, art. 7, comma quarto, lett. b).

Essenziale alla funzionalità del Modello è la predisposizione di un corretto sistema disciplinare; l'eventuale applicazione del sistema sanzionatorio e delle relative sanzioni disciplinari, riferendosi alla violazione di tali regole, è indipendente dal sorgere e dall'esito di un eventuale procedimento penale instaurato dall'autorità giudiziaria. Sono soggetti al sistema tutti i dipendenti, gli amministratori nonché tutti coloro che abbiano rapporti contrattuali con la Società.

Ogni violazione del Modello o delle procedure stabilite in attuazione dello stesso, da chiunque commessa, deve essere immediatamente comunicata per iscritto all'Organismo di Vigilanza da parte dei destinatari del presente Modello, ferme restando le procedure e i provvedimenti di competenza del titolare del potere disciplinare. Conseguentemente, la valutazione rispetto all'applicazione del sistema disciplinare viene effettuata anche nei confronti di chiunque violi tali misure, o effettui, con dolo o colpa grave, segnalazioni che si rivelino infondate.

L'Organismo di Vigilanza deve immediatamente dare corso ai necessari accertamenti, garantendo la riservatezza del soggetto nei cui confronti deve procedere.

L'Organismo di Vigilanza attraverso strumenti ritenuti i più idonei, verifica il flusso di informazione e formazione circa l'esistenza ed il contenuto del sistema disciplinare.

La gestione dei procedimenti disciplinari deve, in ogni caso, rispettare le caratteristiche di status giuridico del soggetto nei cui confronti si procede.

### ***Applicabilità nei confronti di operai, impiegati e quadri aziendali***

Il sistema disciplinare aziendale si fonda sulle norme previste in materia dal Codice Civile, dallo Statuto dei Lavoratori, dal CCNL di categoria e in ogni caso dalla normativa applicabile in materia.

Le sanzioni applicabili nei riguardi di operai, impiegati e quadri sono quelle previste dal CCNL industria alimentare applicato in azienda, ovvero:

1. richiamo verbale;
2. ammonizione scritta;
3. multa fino ad un importo pari a tre ore di retribuzione calcolata sul minimo tabellare;
4. sospensione dal lavoro e dalla retribuzione fino a un massimo di tre giorni;
5. licenziamento con preavviso;
6. licenziamento senza preavviso.

Il sistema, come previsto anche dal CCNL di categoria, esemplifica i comportamenti disciplinarmente rilevanti in base al rilievo che assumono le singole fattispecie, elencando le sanzioni applicabili sulla base della loro gravità. Ad integrazione dell'esemplificazione prevista dal CCNL di categoria e quale ulteriore esemplificazione, si precisa che incorre in un illecito il lavoratore che anche attraverso condotte omissive ed in eventuale concorso con altri:

- a) violi le procedure interne previste dal presente Modello per "inosservanza delle disposizioni di servizio";
- b) violi le procedure interne previste dal presente Modello ponendo in essere un comportamento consistente in "tolleranza di irregolarità di servizi" ovvero in "inosservanza di doveri o obblighi di servizio, da cui non sia derivato un pregiudizio al servizio o agli interessi della Società";
- c) violi le procedure interne previste dal presente Modello o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, ove in tali comportamenti sia ravvisabile un "rifiuto di eseguire ordini concernenti obblighi di servizio", ovvero una "abituale negligenza o abituale inosservanza di leggi o regolamenti o

obblighi di servizio nell'adempimento della prestazione di lavoro", ovvero, in genere, qualsiasi negligenza o inosservanza di leggi o regolamenti o degli obblighi del servizio deliberatamente commesse e non altrimenti sanzionabili;

- d) adottati nell'espletamento delle attività nelle aree a rischio un comportamento non conforme alle prescrizioni del presente Modello, nel caso in cui in tale comportamento sia ravvisabile una "irregolarità, trascuratezza o negligenza, oppure per inosservanza di leggi, regolamenti o degli obblighi di servizio da cui sia derivato un pregiudizio alla sicurezza ed alla regolarità del servizio, con gravi danni ai beni di CIO o di terzi";
- e) adottati nell'espletamento delle attività nelle aree a rischio un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico di CIO di misure previste dal Decreto, dovendosi ravvisare in tale comportamento una "violazione dolosa di leggi o regolamenti o di doveri d'ufficio che possano arrecare o abbiano arrecato forte pregiudizio a CIO o a terzi";
- f) abbia posto in essere un comportamento diretto alla commissione di un reato previsto dal D.Lgs. 231/2001.

È previsto il necessario coinvolgimento dell'Organismo di Vigilanza nella procedura di accertamento delle violazioni e di irrogazione delle sanzioni per violazione del Modello, nel senso che non potrà essere archiviato un provvedimento disciplinare ovvero irrogata una sanzione disciplinare, per violazione del Modello, senza darne immediata informazione e, ove richiesto dal titolare del potere disciplinare, senza aver ottenuto il parere dell'Organismo di Vigilanza.

Con la contestazione, può essere disposta la revoca delle eventuali procure affidate al soggetto interessato.

Il tipo e l'entità delle richiamate sanzioni saranno valutate anche in funzione:

- al grado di negligenza, imprudenza o imperizia in funzione alla prevedibilità dell'evento;
- agli incarichi, posizione funzionale e responsabilità delle persone coinvolte nei fatti.

#### **Applicabilità nei confronti degli amministratori e collegio sindacale**

Il presente Modello viene consegnato a ciascun componente del Consiglio d'Amministrazione e al Collegio Sindacale.

Quando la violazione delle procedure interne previste dal Modello è compiuta da parte di Amministratori e Sindaci, l'OdV informerà l'intero Consiglio d'Amministrazione e il Collegio Sindacale, i quali provvederanno ad applicare, nei confronti dei responsabili, le iniziative ritenute più idonee in conformità a quanto previsto dalla normativa in materia.

Le sanzioni di natura disciplinare, nonché l'eventuale richiesta di risarcimento dei danni, verranno commisurate al livello di responsabilità, al ruolo ed all'intensità del vincolo fiduciario correlato all'incarico conferito.

#### **Applicabilità nei confronti di ogni altro soggetto che intrattenga rapporti con CIO**

CIO ha, tra l'altro, previsto l'applicazione del proprio Modello anche nei confronti dei Business Partners. Si prevede, ad esempio:

- l'inserimento nei propri contratti, ivi compresi gli ordini di acquisto, di clausole che attribuiscono a CIO la facoltà, ove lo ritenga opportuno, di risolvere il contratto, nel caso in cui alla controparte venga ascritto (anche solo in via "cautelare") uno dei "reati presupposto" contemplati dal D. Lgs 231/2001;
- l'inserimento nei contratti di prestazione intellettuale, ove possibile, della facoltà di recesso *ad nutum*, ossia della facoltà di recedere non solo, ma anche, per ragioni di *Compliance*.

## **12. Formazione e diffusione del modello organizzativo CIO**



Ai fini dell'efficacia del presente Modello, è obiettivo di CIO garantire una corretta conoscenza e divulgazione delle norme di comportamento ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle attività sensibili.

L'adozione del Modello, ed i relativi aggiornamenti, sono comunicati ai dipendenti ed agli stakeholders al momento dell'approvazione.

Il Modello viene portato a conoscenza nella sua versione integrale ai dipendenti, mentre sul sito internet viene pubblicato soltanto il codice etico, parte integrante dei rapporti contrattuali aziendali.

Ai nuovi assunti viene consegnato un pacchetto informativo disponibile portale aziendale o consegnato in modo cartaceo a chi non aderisce al sistema informatizzato di gestione delle informazioni (CCNL, Codice Etico, Codice Disciplinare, Informativa privacy e sicurezza/salute, ...), con il quale si assicura agli stessi le conoscenze considerate fondamentali in Azienda. Attraverso la firma originale e/o l'accesso al portale è possibile tracciare la lettura e presa visione dei documenti disponibili che attestano la ricezione del pacchetto informativo, nonché l'integrale conoscenza dei documenti allegati e l'impegno ad osservarne le prescrizioni.

L'attività di formazione è finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 e successive modifiche ed integrazioni, spiegare i motivi per cui CIO ha deciso di dotarsi di un Modello nonché ad illustrare i principali comportamenti da adottare al fine di prevenire la commissione dei Reati; annualmente il piano della formazione viene definito ed approvato dall'Organismo di Vigilanza ed erogato dai suoi membri che aggiornano il CDA in merito al suo rispetto.