Modello Organizzativo ai sensi del

Decreto Legislativo 8 giugno 2001, n. 231

REV.	DATA	STORIA DEL DOCUMENTO
0	22.9.2021	PRIMA EMISSIONE

Adottato dal Consiglio di Amministrazione di CY4GATE S.p.a.

il 22.9.2021

SOMMARIO

PARTE GENERALE

SEZIONE PRIMA

IL DECRETO LEGISLATIVO 231/2001

1.1 La Responsabilità amministrativa degli enti

In data 8 giugno 2001 è stato emanato - in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 - il Decreto Legislativo 8 maggio 2001 n. 231 (di seguito denominato anche il "Decreto" o "D. Lgs. 231/2001"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia aveva già da tempo aderito, ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione di funzionari della Comunità Europea o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Il Decreto ha introdotto nell'ordinamento giuridico la responsabilità amministrativa degli enti per gli illeciti dipendenti da reato. Le disposizioni in esso previste si applicano agli *"enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica"* (di seguito anche solo "enti').

Tale nuova forma di responsabilità, sebbene definita "amministrativa" dal legislatore, presenta tuttavia taluni caratteri propri della responsabilità penale, essendo ad esempio rimesso al giudice penale competente l'accertamento dei reati dai quali essa deriva ed essendo estese all'ente le garanzie del processo penale.

***

Nello specifico, in via innovativa rispetto al passato, il Decreto 231/2001 stabilisce che ogni ente, con o senza personalità giuridica e con la sola eccezione di alcuni enti di rilievo pubblicistico, è potenzialmente soggetto alle sanzioni dal medesimo decreto previste qualora:

- sia stato commesso un reato rientrante tra quelli significativi da parte di soggetti appartenenti all'ente e, cioè: da (i)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 persone che esercitano, anche di fatto, la gestione ed il controllo della stessa (c.d. soggetti o persone apicali); (ii) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera (i);
- il reato commesso rientri tra quelli tassativamente elencati nel predetto Decreto. Pur non essendo ricompresi formalmente nel Decreto, la responsabilità amministrativa-penale delle società è stata estesa anche ai reati transnazionali previsti dalla Legge 16 marzo 2006 n. 146 e, quindi, alle fattispecie delittuose concernenti l'associazione per delinquere, di natura semplice o mafiosa, il riciclaggio, il traffico di migranti e l'intralcio alla giustizia, purché commesse in più di uno Stato.

L'ente non può essere ritenuto responsabile se le persone sopra indicate hanno agito nell'interesse esclusivo proprio o di terzi.

Oltre all'esistenza degli elementi oggettivi e soggettivi sopra descritti, il D.Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è in definitiva riconducibile ad una "colpa di organizzazione", da intendersi quale mancata adozione, da parte dell'ente, di misure adeguate a prevenire la commissione dei reati elencati al successivo paragrafo, da parte dei soggetti individuati nel Decreto.

La responsabilità amministrativa dell'ente è, quindi, ulteriore e diversa da quella della persona fisica che ha, materialmente, commesso il reato. Entrambe costituiscono oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o non risulti punibile.

La responsabilità dell'impresa può ricorrere anche se il delitto presupposto si configura nella forma di tentativo (ai sensi dell'art. 26 del D. Lgs. 231/2001), vale a dire quando il soggetto agente compie atti idonei diretti in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica.

Ai sensi degli articoli 5 e 6 del Decreto 231/2001, sono fattori costitutivi del c.d. scudo protettivo:

- l'adozione e l'efficace attuazione, prima della commissione del reato, di un documento complesso interno definito modello di organizzazione e gestione, quale ambisce essere il presente atto, idoneo a svolgere, secondo i criteri normativi applicabili, adeguata azione preventiva rispetto alla commissione dei reati della specie di quello verificatosi;
- la nomina e l'operatività di un precisato organismo dell'ente (c.d. Organismo di Vigilanza) dotato di autonomi poteri di

iniziativa e di controllo, avente il compito di vigilare sul funzionamento e l'osservanza del predetto modello di organizzazione e gestione e di curare il suo aggiornamento.

Per ciò che attiene al rapporto tra soggetti c.d. apicali e modello, è importante sottolineare come nel caso concreto l'ente deve altresì, al fine di non incorrere in responsabilità, dimostrare in giudizio, nel caso di azione avversa: (i) che nel commettere il reato costoro si siano volontariamente e fraudolentemente sottratti alle prescrizioni contenute nel modello; (ii) che non vi sia stata omessa o insufficiente sorveglianza da parte dell'Organismo di Vigilanza .

Per entrambi i primi due fattori costitutivi del modello si impone, quindi, una piena dimostrazione di concreta operatività, anche in via di fatto. Risulteranno, inoltre, decisive le circostanze reali del fatto di reato.

Relativamente ai soggetti non apicali, la presenza del modello esclude, presuntivamente (e ciò non va quindi dimostrato caso per caso), ogni forma di responsabilità amministrativo-penale dell'ente. E', in tale ipotesi, l'Autorità procedente ad avere l'onere processuale di provare l'eventuale inadeguatezza ed inidoneità del modello medesimo.

***

Il presente documento costituisce la formalizzazione concreta del Modello della Cy4gate ed è il frutto di un'apposita attività di analisi condotta all'interno della Società, con il precipuo scopo di dotarla dell'idoneo strumento citato, realizzato per essere in grado di

affrancare la medesima dall'applicazione delle regole sanzionatorie di responsabilità amministrativa previste dal Decreto 231/2001.

L'adeguatezza del Modello è, pertanto, assicurata dalla sua aderenza e coerenza con la realtà aziendale regolamentata, cui ogni prescrizione del documento è riferita.

In tale ottica, l'elaborazione del Modello e la definizione delle sue componenti normative sono connesse alle risultanze aziendali relative alla struttura organizzativa della Società, nonché alla normativa di riferimento ed ai rischi giuridici riconducibili alla conduzione delle operazioni tipiche del settore economico interessato.

A tal riguardo, sono state effettuate (a) apposite interviste conoscitive nei confronti di talune delle principali funzioni aziendali nonché (b) l'analisi della documentazione specifica riguardante la situazione organizzativa ed economica della Società ed, infine, (c) l'analisi dell'apparato di procedure e del connesso sistema di controlli di cui la Società si è già dotata.

In particolare, tali attività conoscitive hanno riguardato da un lato l'articolato sistema di procedure e controlli di cui alla normativa interna, ed il sistema di controllo contabile affidato ad apposita Società di Revisione esterna, il sistema di controllo interno di gestione ed il sistema di controllo adottato ai fini della sicurezza del lavoro (Documento di Valutazione dei Rischi).

All'esito di tali verifiche, si è ritenuto opportuno creare una struttura del Modello che - in un'ottica di ottimizzazione delle risorse sociali ed anche al fine di ottenere un virtuoso contenimento dei costi e i benefici derivanti alla Società dal proprio adeguamento al sistema di organizzazione e gestione di cui al Decreto 231/2001 - fosse in grado di recepire i meccanismi di *compliance* già in essere presso la

Società, adeguandoli e/o integrandoli ove necessario rispetto alle finalità di cui al medesimo Decreto 231/2001.

Pertanto, il Modello della Cy4gate costituisce in primo luogo uno strumento di raccordo tra i processi, le misure e le procedure operative di cui la Società si è già dotata (valorizzandoli appunto anche ai fini del Decreto 231/2001) e, in secondo luogo, ove necessario ed al fine di regolamentare eventuali aree di rischio risultate non sufficientemente controllate dai predetti sistemi già presenti, un sistema di nuove ed opportune regole utili al miglioramento ed al completamento dell'apparato organizzativo interno. Conseguentemente il Modello, oltre che intervenire direttamente nelle aree non monitorate dai predetti *advisors*, realizza un coordinamento tra gli attuali responsabili (interni o esterni) del controllo (*advisors*), con conseguenti proficue sinergie. A tale ultimo scopo, è previsto che l'Organismo di Vigilanza, nello svolgimento delle funzioni sue proprie come definite dall'art. 6 del Decreto 231/2001, sia coadiuvato - quale organo referente e soggetto collettore delle rispettive attività, istanze e segnalazioni - dagli *advisors* e dagli altri attori del controllo interno ed esterno con i quali si relaziona.

1.2 I reati previsti dal Decreto

I reati, dal cui compimento può derivare la responsabilità amministrativa dell'ente sono quelli, espressamente, richiamati dal D. Lgs. 231/2001, e successive modifiche ed integrazioni.

Si elencano di seguito le "famiglie di reato", attualmente, ricomprese nell'ambito di applicazione del D. Lgs. 231/2001:

1. **Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea per il**

conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D. Lgs. n. 231/2001) [articolo modificato dalla dlgs 75 del 24 luglio 2020].

2. **Delitti informatici e trattamento illecito di dati** (Art. 24-bis, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D. Lgs. n. 7 e 8/2016].
3. **Delitti di criminalità organizzata** (Art. 24-ter, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. n. 69/2015 e dalla L. 236/2016]
4. **Peculato, concussione, induzione indebita a dare o promettere altra utilità, corruzione e abuso d'ufficio** (Art. 25, D. Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012 e dal D. lgs 75/2020].
5. **Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** (Art. 25-bis, D. Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D. Lgs. n. 125/2016].
6. **Delitti contro l'industria e il commercio** (Art. 25-bis.1, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009].
7. **Reati societari** (Art. 25-ter, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. n. 69/2015, dal D. Lgs. n. 38/2017].
8. **Reati con finalità di terrorismo o di eversione dell'ordine democratico** previsti dal codice penale e dalle leggi speciali (Art. 25-quater, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2003].

9. **Pratiche di mutilazione degli organi genitali femminili** (Art. 25-quater.1, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2006].
10. **Delitti contro la personalità individuale** (Art. 25-quinquies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016].
11. **Reati di abuso di mercato** (Art. 25-sexies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005].
12. **Altre fattispecie in materia di abusi di mercato** (Art. 187-quinquies TUF) [articolo modificato dal D. Lgs. n. 107/2018].
13. **Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro** (Art. 25-septies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007; modificato dalla L. n. 3/2018].
14. **Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (Art. 25-octies, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014].
15. **Delitti in materia di violazione del diritto d'autore** (Art. 25-novies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009].
16. **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (Art. 25-decies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009].
17. **Reati ambientali** (Art. 25-undecies, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 121/2011 e modificato dalla L. 68/2015, modificato dal D. Lgs. n. 21/2018 e D. lgs 116/2020].

18. **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (Art. 25-duodecies, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 109/2012, modificato dalla L. n. 161/2017].
19. **Reati di razzismo e xenofobia** (Art. 25-terdecies, D. Lgs. 231/2001) [articolo aggiunto dalla L. n. 167/2017, modificato dal D. Lgs. n. 21/2018].
20. **Frode in competizioni sportive, esercizio di gioco o di scommessa, giochi di azzardo esercitati a mezzo di apparecchi vietati** (Art. 25 quaterdecies, D. Lgs. 231/2001- L. 39/2019).
21. **Reati tributari** (art. 25 quinquiesdecies, D.lgs 231/2001, articolo aggiunto dall'art. 39, comma 2, della legge n. 157 del 2019 e ampliato dal D.lgs n.75/2020).
22. **Reati transnazionali** (L. n. 146/2006) pur non essendo ricompresi formalmente nel Decreto 231/2001, la responsabilità amministrativa-penale delle società è stata estesa anche ai reati transnazionali previsti dalla Legge 16 marzo 2006 n. 146 e, cioè, alle fattispecie delittuose concernenti l'associazione per delinquere, di natura semplice o mafiosa, il riciclaggio, il traffico di migranti e l'intralcio alla giustizia, purché commesse in più di uno Stato.
23. **Reati di contrabbando** (art. 25 sexiesdecies D.lgs. 231/2001- articolo aggiunto dal D. lgs. n. 75/2020).

1.3 I reati commessi all'estero

In forza dell'articolo 4 del Decreto, l'ente può essere considerato responsabile, in Italia, per la commissione all'estero di taluni reati. In particolare, l'art. 4 del Decreto prevede che gli enti aventi la sede

principale nel territorio dello Stato rispondono anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Pertanto, l'ente è perseguibile quando:

- in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (enti privi di personalità giuridica);
- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;
- la richiesta del Ministro della giustizia, cui sia eventualmente subordinata la punibilità, è riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Per le condotte criminose, che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità *ex* art. 6 del codice penale, in forza del quale "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

1.4 Le sanzioni previste dal Decreto

La competenza a conoscere degli illeciti amministrativi dell'ente appartiene al giudice penale. L'accertamento della responsabilità può comportare l'applicazione di sanzioni gravi e pregiudizievoli per la vita dell'ente stesso, quali:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

L'ammontare delle sanzioni pecuniarie varia a seconda: (i) della gravità del fatto, (ii) del grado della responsabilità dell'ente, (iii) dell'attività, eventualmente, svolta dall'ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti, (iv) delle condizioni economiche e patrimoniali dell'ente.

Le sanzioni interdittive, che si applicano in relazione ai reati per i quali sono espressamente previste, possono comportare importanti restrizioni all'esercizio dell'attività di impresa dell'ente, quali:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione, salvo che per le prestazioni del pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Tali misure possono essere applicate all'ente anche in via cautelare e, dunque, prima dell'accertamento nel merito in ordine alla sussistenza del reato e dell'illecito amministrativo che da esso dipende, nell'ipotesi in cui si ravvisi l'esistenza di gravi indizi tali da far ritenere la responsabilità dell'ente, nonché il pericolo di reiterazione dell'illecito.

Nell'ipotesi in cui il giudice ravvisi l'esistenza dei presupposti per l'applicazione di una misura interdittiva a carico di un ente che svolga attività di interesse pubblico, ovvero abbia un consistente

numero di dipendenti, lo stesso potrà disporre che l'ente continui a operare sotto la guida di un commissario giudiziale.

L'art. 1 comma 9, della Legge n. 3 del 2019 ha modificato il comma 2 dell'art. 13 del D. Lgs. 231/2001, stabilendo che le sanzioni interdittive abbiano una durata non inferiore a tre mesi e non superiore a due anni, fermo restando il disposto dell'art. 25 comma V del medesimo decreto legislativo, che prevede più gravi sanzioni interdittive nei casi di condanna per uno dei delitti di cui agli articoli 317, 319,319 -bis, 319-ter, comma 1 e 2, 319-quater, 321, 322, commi 2 e 4, del codice penale.

1.5 Condizione esimente della responsabilità amministrativa

L'art. 6 del D. Lgs. 231/2001 stabilisce che l'ente, nel caso di reati commessi da soggetti apicali, non risponda qualora dimostri che:

- l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (c.d. "Organismo di Vigilanza, nel seguito anche "Organismo" o "O.d.V.");
- le persone hanno commesso il reato eludendo fraudolentemente il suddetto Modello;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso in cui il reato sia stato commesso da soggetti sottoposti alla direzione o alla vigilanza del personale apicale, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di inosservanza degli obblighi di direzione e vigilanza.

Pertanto, l'ente che, prima della commissione del reato, adotti e dia concreta attuazione ad un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, va esente da responsabilità se risultano integrate le condizioni di cui all'art. 6 del Decreto.

In tal senso il Decreto fornisce specifiche indicazioni in merito alle esigenze cui i Modelli 231 devono rispondere e, cioè:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi i reati previsti dal predetto Decreto;
- prevedere specifici "protocolli" diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati sopra citati;
- prevedere obblighi di informazione nei confronti dell'O.d.V.;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Tuttavia la mera adozione di un Modello di Organizzazione, Gestione e Controllo non è di per sé sufficiente ad escludere detta responsabilità, essendo necessario che lo stesso sia effettivamente ed efficacemente attuato. In particolare ai fini di un’efficace attuazione del modello, il Decreto richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando siano emerse significative violazioni delle prescrizioni,

ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;

- la concreta applicazione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello stesso.

SEZIONE SECONDA

IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI CY4GATE

PREMESSA

Cy4gate opera nel settore della progettazione, sviluppo e produzione di tecnologie, prodotti e servizi finalizzati a soddisfare le esigenze di cyber intelligence, cyber security e cyber electronic warfare concernenti le forze armate, le forze di polizia e le agenzie di intelligence e, per quanto concerne la sola cyber security, quelle proprie di soggetti privati.

L'offerta commerciale della società si ripartisce, pertanto, nelle due macroaree di cyber intelligence e cyber security.

Con riferimento alla prima, la Società realizza programmi volti alla raccolta ed analisi delle informazioni presenti online e veicolate tramite la rete internet, nonché la raccolta di informazioni prodotte mediante l'utilizzo di dispositivi elettronici e digitali. Con riferimento alla seconda, la Società realizza prodotti di cybersecurity, finalizzati alla protezione dei sistemi informatici dei propri clienti, ma anche all'analisi ed alla catalogazione delle minacce, proponendo misure di contrasto.

Cy4gate adotta il modello di amministrazione e controllo tradizionale, che risulta adeguato a perseguire l'obiettivo di un appropriato bilanciamento dei poteri ed una puntuale distinzione

delle funzioni: (i) di supervisione strategica, affidata al Consiglio di Amministrazione; (ii) di gestione, demandata all'Amministratore Delegato; (iii) di controllo, svolta dal Collegio Sindacale.

In particolare:

il Consiglio di Amministrazione vigila sul generale andamento della gestione tenendo in considerazione le informazioni ricevute dall'Amministratore delegato. Esamina ed approva le operazioni ordinarie e straordinarie, nonché i piani strategici della società. Provvede a valutare ed approvare la documentazione di rendiconto periodico;

l'Amministratore delegato fissa le linee strategiche della società. Esamina i principali rischi della società derivanti dal Sistema di risk management aziendale approvando le azioni di mitigazione. Definisce gli strumenti e le modalità di attuazione del controllo interno;

il Collegio sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e, in particolare, sull'adeguatezza dell'assetto organizzativo amministrativo e contabile adottato dalla Società e sul suo concreto funzionamento.

L'assemblea elegge il collegio sindacale, costituito da un minimo di 3 (tre) ad un massimo di 5 (cinque) sindaci effettivi e 2 (due) supplenti, ne nomina il presidente e determina per tutta la durata dell'incarico il compenso dei presenti. I sindaci scadono alla data dell'assemblea convocata per l'approvazione del bilancio relativo al terzo esercizio della carica. La cessazione dei sindaci per scadenza del termine ha effetto dal momento in cui il collegio è stato ricostituito.

La Società è sottoposta all'attività di **revisione legale** dei conti della KPMG.

La suddetta società, oltre a svolgere l'attività di revisione legale dei bilanci d'esercizio si occupa della revisione contabile del financial reporting package, al fine di valutare l'appropriatezza dei principi contabili adottati, nonché di valutare la correttezza dei bilanci d'esercizio annuali.

L'attività di controllo contabile è annotata nell'apposito libro conservato presso la sede sociale.

2.1 Contesto organizzativo interno ed aree di funzione.

La Società è ripartita in aree aziendali dotate di una rete di procedure interne strutturate, sottoposte al controllo esercitato dal Collegio Sindacale e, in genere, dall'Organo amministrativo, nonché dalla società di revisione contabile.

Le risorse umane della Società sono ripartite nelle seguenti principali aree.

(a) Area Finance.

E' assegnata alla responsabilità del Chief Financial Officer (CFO). Assicura il ciclo di pianificazione e budget aziendale, le attività di controllo, amministrazione (contabilità generale e bilancio civilistico), fiscale e tesoreria; la valutazione ed implementazione di operazioni straordinarie; le attività di investor relations verso investitori istituzionali e Borsa Italiana.

La mission della Funzione Finance è assicurata dalle seguenti unità organizzative: Accounting & Tax; Planning & Controlling.

Il Chief Financial Officer ha il ruolo, tra l'altro, di Investor Relator, con la responsabilità della gestione della comunicazione economico-finanziaria della Società e delle relazioni con agenzie di rating, broker e stakeholder finanziari.

(b) Area Human Resources, Legal & Corporate Shared Services.

Human Resources si occupa di tutte le attività inerenti alle politiche del personale e di sviluppo organizzativo, nonchè della gestione amministrativa. Integra le strategie e politiche HR, garantendo un processo di selezione e reclutamento del personale qualitativamente e quantitativamente idoneo al raggiungimento degli obiettivi aziendali.

Legal & Security assicura la tutela degli interessi aziendali attraverso l'analisi dei testi contrattuali e degli accordi, anche avvalendosi del supporto di advisor esterni. Si occupa, tra l'altro, dell'aggiornamento, del modello organizzativo ex legge 231, delle policy di CSR e garantisce il presidio del Sistema di Gestione per la Privacy.

Quality assicura la gestione del sistema di qualità aziendale ed implementa un sistema di continous improvement al fine di sviluppare miglioramenti per l'Azienda in tutti i principali aspetti organizzativi.

Plant Management si occupa dello sviluppo del business aziendale. Gestisce le risorse energetiche e l'erogazione dei servizi per lo stabilimento. Assicura la tutela della salute e della sicurezza del personale e la gestione di tutte le trasferte aziendali.

A supporto del Chief Extecutive Officer opererà il Senior Advisor, coadiuvandolo nell'individuazione delle linee di crescita e sviluppo dell'azienda, nell'implementazione di modelli comunicativi e di marketing funzionali al consolidamento del brand e mello sviluppo del network relazionale con particolare riferimento a FF.AA., FF.PP., Agenzia di Intelligence, Istituzioni e Industrie.

(c)Area Marketing & Sales.

E' responsabile, anche tramite il ruolo del Chief Commercial Officer (CCO), del presidio commerciale dei clienti/mercati. In particolare la funzione assicura le attività di business development, di promozione dei prodotti della società, dell'acquisizione degli ordini secondo i piani e gli obiettivi aziendali, della gestione del cliente e della definizione degli accordi commerciali. Massimizza, altresì, le opportunità di crescita del business aziendale tramite accordi di partnership e collaborazione con clienti, partner e system integrator.

Condivide con le altre Funzioni aziendali la responsabilità del raggiungimento dell'Order Intake di Budget alle redditività attese.

Il CCO si avvale della collaborazione delle figure dell'International sales Managers e del Domestic Sales Manager come Marketing Specialist.

(d) Area Engineering.

Ha la missione, tramite anche la figura del Chief Technical Officer, di presidiare il costante sviluppo dell'innovazione aziendale (research and development), gestire l'evoluzione dei prodotti, garantire (in collaborazione con la funzione ,
s) la gestione dei programmi in corso e delle delivery contrattuali, assicurando lo sviluppo efficiente/efficace delle attività di ingegneria in termini di tempi, costi, qualità, affidabilità e prestazioni. Ha inoltre la responsabilità della gestione dei sistemi informativi aziendali, dello sviluppo delle architetture HW/IT dei prodotti della società e dei servizi post-vendita.

Definisce la politica di make or buy al fine di consolidare ed ampliare il portfolio di soluzioni in maniera efficace. Garantisce la corretta esecuzione dei processi di verifica delle piattaforme durante tutte le fasi del processo di Sviluppo.

Le unità ricomprese all'interno di tale Area sono:

Cyber Intelligence che, tramite il Head of Cyber Intelligence, progetta ed implementa i prodotti di Decision Intelligence dell' Azienda, utili a supportare i processi decisionali di clienti governativi e corporate.

Cyber Security che, tramite il Head of Cyber Security, progetta e sviluppa prodotti di Cyber Security per il mercato corporate e governativo.

Cyber Analysis che, tramite la figura del Head of Cyber Analysis, assicura lo sviluppo, implementazione e evoluzione dei tool di Lawful Interception necessari as assicurare le performance richieste dagli end user.

Cyber Humint che, tramite la figura del Head of Cyber Humint, assicura l'implementazione ed evoluzione dei prodotti di Human Intelligence.

Cyber Support che, tramite la figura del Head of Cyber Support, ha la responsabilità di garantire il costante presidio del cliente nazionale nelle attività di Cyber Analysis.

Information Technology che, tramite la figura del Head of Information Technology, coordina e implementa le infrastrutture tecnologiche aziendali compresi la rete dati, i server e i servizi di posta elettronica.

(e) Area Technical Marketing and Pre Sales.

Si occupa, tramite il ruolo del Chief scientist Officer, delle attività di prevendita e supporto alle vendite per la proposizione tecnica di scouting, benchmarking tecnologico ed analisi di mercato e di coordinamento tecnico per le proposte di finanziamento per la ricerca e innovazione. Supporta la funzione Sales & Marketing relativamente a presentazioni tecniche, identificazioni architetture e servizi a sostegno della proposta commerciale e redazione degli allegati tecnici. Supporta la Funzione Programs, in collaborazione

con Engineering, nella definizione e validazione dei contenuti dei corsi da offrire ai clienti, proponendo e qualificando docenti interni ed esterni sia per i servizi di Academy che Digilab. Offre supporto tecnico/scientifico alle iniziative promozionali come conferenze, social network, articoli e contenuti tecnici.

(f) Area Programs & Sourcing Management, tramite la figura del Chief Programs & Sourcing Management Officer, assicura il rispetto degli impegni contrattuali assunti in termini di tempi, costi e qualità attesa della fornitura con una gestione "end to end" dei programmi aziendali. Approvvigiona i materiali ed i servizi necessari per la realizzazione delle commesse e dei prodotti. A tal fine operano: l'**Unità Programs** che, tramite il Program Manager, ha la responsabilità di realizzare i risultati a budget e si occupa dei processi di gestione e controllo del ciclo di vita dei Programmi firm, nonchè della gestione del rapporto con il Cliente a garanzia degli impegni assunti per il mantenimento di un ottimale livello di soddisfazione del Cliente. Vi è poi l'**Unità Sourcing Management** che, tramite i Procurement Specialist, ha la responsabilità di operare a supporto dell'intero Product Life Cycle, a partire dalla definizione dell'offerta fino alla gestione delle forniture nella fase di post- vendita. Supporta, altresì, le scelte di Make or Buy e presidia il mercato di fornitura tramite un continuo Scouting tecnologico per attivare relazioni di collaborazione con fornitori strategici allo scopo di rendere disponibili tecnologie e prodotti e ridurre il time to market.

2.2 Sistema di controllo interno di gestione

Il sistema interno di controllo di gestione (SCG) e reporting è stato costruito per monitorare l'andamento economico della Società e si basa su una impostazione di un processo interno di pianificazione e

controllo che permette di definire e analizzare, per ogni ciclo di pianificazione (budget, forecast e consuntivo), i Key Perfomance indicators della Società, impostando le necessarie azioni per il recupero degli scostamenti.

A guida del processo di pianificazione e controllo sono formalizzate ed attuate le seguenti procedure:

- processo forecasting e consuntivazione, in cui è definito il calendario amministrativo per le chiusure mensili relative alle attività di progetti in essere;
- ciclo di pianificazione- controllo- reporting, in cui sono definite le linee guida per la produzione dei documenti di pianificazione, controllo e reporting aziendale.

Il sistema interno di controllo di gestione e reporting è stato sottoposto ad attenta due diligence da parte di KPMG in sede di IPO della Società a giugno 2020.

2.3 Sistema di gestione della Qualità

L'attività svolta dalla Società è, altresì, sottoposta ad una serie di controlli derivanti dall'applicazione delle procedure sulla qualità.

Attraverso tale sistema di gestione della qualità, in particolare, un ente esterno (l'Organismo di Certificazione) certifica che il sistema interno di gestione della Società è organizzato secondo determinate, corrette ed efficaci norme di comportamento, nonché secondo un determinato sistema di suddivisione di responsabilità e controlli, il cui rispetto comporta il raggiungimento di determinati obiettivi sul mercato.

Cy4gate ha ottenuto la certificazione ISO9001:2015, che contraddistingue un preciso e dettagliato modo di operare

dell'azienda, idoneo a fornire un prodotto ed un servizio di qualità con riferimento ai seguenti settori:

- progettazione, realizzazione ed assistenza post-vendita di software e soluzioni ICT, anche fondate su tecnologie di artificial intelligence, per il mercato della cyber security, del big data analytics e dei processi di digitalizzazione e automazione;
- fornitura di prodotti di cyber security, inclusivi della formazione di ruoli specialistici per il loro impiego in teamwork organizzato;
- erogazione di servizi di security operation center (SOC);
- real time monitoring e supporto per l'incident response;
- commercializzazione di prodotti SW e HW ICT per clienti pubblici e privati.

Cy4gate ha ottenuto la certificazione ISO9001:2015 nei seguenti settori IAF:

- 29a. commercio all'ingrosso, al dettaglio e intermediari del commercio;
- 33. tecnologia dell'informazione;
- 37. istruzione.

2.4 Audit sui sistemi di gestione di Cy4gate

Cy4gate, in particolare, conduce ad intervalli pianificati *audit* interni prendendo in considerazione lo stato e l'importanza dei processi e delle aree da sottoporre ad *audit*.

Cy4gate ha definito i criteri, il campo di applicazione, la frequenza ed i metodi dell'*audit*.

I metodi prevedono:

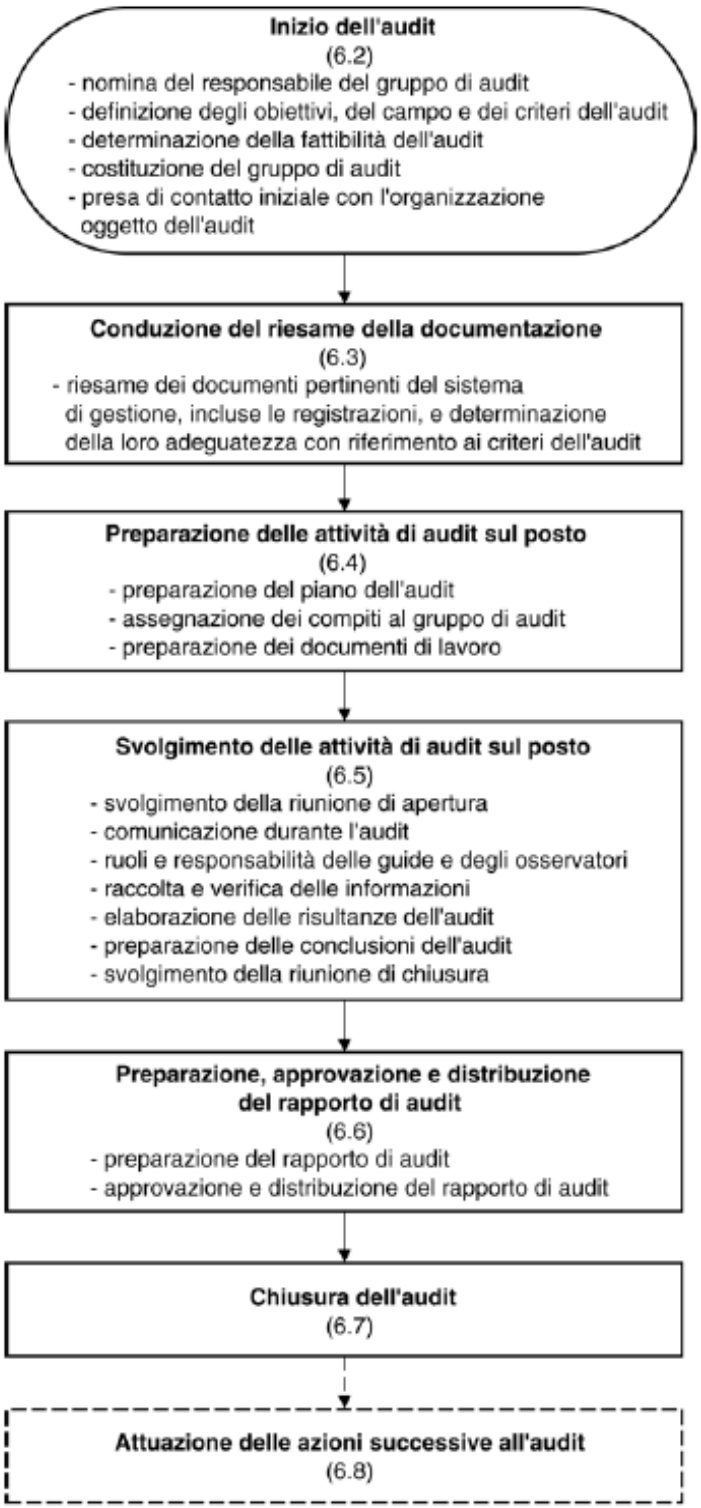
- verifica a campione sulle attività riferite a tutti i processi aziendali per valutarne la conformità alle procedure definite;
- verifica a campione sull'efficacia dei controlli effettuati sulle attività (autocontrollo, controllo a cura del responsabile di reparto, controllo da applicativi software - quando applicabile);
- verifica a campione sull' efficacia delle attività di audit (capacità degli audit di intercettare anomalie o carenze o eventi comunque non conformi alle regole stabilite e documentate tramite procedure o altri documenti).

La Società si sottopone, nei termini indicati, ad Audit specifici in relazione alla (i) revisione legale ed al controllo legale dei conti; (ii) al mantenimento del Sistema della Qualità aziendale ISO 9001:2015.

Le verifiche sono condotte, per quanto concerne il punto (i) da Kpmg come da piano di revisione, e dal Collegio sindacale con cadenza trimestrale ed in occasione dell'approvazione del bilancio; per quanto concerne il punto (ii) dall'Ente di certificazione del Sistema con cadenza annuale per il mantenimento della certificazione (l'ultimo audit di sorveglianza è stato eseguito da RINA in data 15/06/2021) e con cadenza triennale per il rinnovo (previsto per il 2022).

I risultati degli Audit inerenti al sistema Qualità sono registrati e archiviati sul portale RINA e, conseguentemente, sull'intranet aziendale Cy4gate.

Di seguito si riporta il flowchart che descrive lo svolgimento di un audit.


Inizio dell'audit
(6.2)
- nomina del responsabile del gruppo di audit
- definizione degli obiettivi, del campo e dei criteri dell'audit
- determinazione della fattibilità dell'audit
- costituzione del gruppo di audit
- presa di contatto iniziale con l'organizzazione oggetto dell'audit
Conduzione del riesame della documentazione
(6.3)
- riesame dei documenti pertinenti del sistema di gestione, incluse le registrazioni, e determinazione della loro adeguatezza con riferimento ai criteri dell'audit
Preparazione delle attività di audit sul posto
(6.4)
- preparazione del piano dell'audit
- assegnazione dei compiti al gruppo di audit
- preparazione dei documenti di lavoro
Svolgimento delle attività di audit sul posto
(6.5)
- svolgimento della riunione di apertura
- comunicazione durante l'audit
- ruoli e responsabilità delle guide e degli osservatori
- raccolta e verifica delle informazioni
- elaborazione delle risultanze dell'audit
- preparazione delle conclusioni dell'audit
- svolgimento della riunione di chiusura
Preparazione, approvazione e distribuzione del rapporto di audit
(6.6)
- preparazione del rapporto di audit
- approvazione e distribuzione del rapporto di audit
Chiusura dell'audit
(6.7)
Attuazione delle azioni successive all'audit
(6.8)

2.5 Altre certificazioni/abilitazioni

1) Cy4gate è in possesso del codice NCAGE (NATO Commercial and Governmental Entity Code).

Tale codice di cinque caratteri alfanumerici, assegnato dall'Organismo Centrale di Codificazione (OCC), identifica:

- un singolo Costruttore e/o Fornitore di articoli di rifornimento che abbia rapporti di tipo contrattuale diretto o indiretto (subfornitore) con l'Amministrazione Difesa (AD) dei Paesi che aderiscono al NATO Codification System (NCS);
- una Ditta, Associazione, persona, ecc. che fornisca servizi alle AD dei Paesi che aderiscono al NCS (Nato Codification System).

2) L'azienda detiene, altresì, la Licenza ex. Art 28 del TULPS per la progettazione, fabbricazione, detenzione e vendita di apparecchiature elettroniche appositamente progettate per uso militare destinate alle FF.AA. e Forze di Polizia, nazionali ed estere.

3) La Società ha ottenuto nel 2020 il NOS (nulla osta sicurezza) che nell'ordinamento italiano rappresenta un'abilitazione al trattamento di informazioni, documenti o materiali classificati dal grado di riservatissimo fino a quello di segretissimo.

4) La Società, infine, ha ottenuto nel 2020 il NOSI (nulla osta sicurezza industriale).

2.6 Finalità del Modello

Cy4gate adotta il presente Modello di organizzazione, gestione e controllo con l'obiettivo di prevenire la commissione dei reati (cd. reati presupposto) da parte di esponenti della Società, apicali o sottoposti all' altrui direzione.

Il presente Modello ha lo scopo di costruire un sistema di controllo interno strutturato e organico, idoneo a prevenire la commissione dei reati previsti dal Decreto.

L'art. 6 del D. Lgs. 231/2001 dispone, espressamente, che i modelli di organizzazione, gestione e controllo possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Nella predisposizione del presente documento la Società osserva, oltre che le prescrizioni del Decreto, delle leggi e regolamenti applicabili, anché gli orientamenti che si stanno consolidando in materia e le *best practices* di *governance* e organizzazione per Società di servizi.

Il Modello che ha predisposto Cy4gate, nel dare attuazione alle indicazioni di cui sopra:

- individua, autonomamente, le specifiche aree di rischio in relazione alla particolare attività svolta, a seguito delle analisi della propria struttura organizzativa e dell'operatività aziendale;
- definisce un sistema normativo interno finalizzato alla prevenzione dei reati nel quale sono tra gli altri ricompresi:
- introduce un codice etico che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali assunti dai dipendenti, amministratori e collaboratori;
- prevede un sistema di deleghe e procure volto ad assicurare una trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
- prevede procedure formalizzate tese a definire ruoli, responsabilità e modalità operative nelle aree a rischio identificate;

- formalizza una struttura organizzativa coerente con gli obiettivi aziendali e le attività da svolgere attraverso la redazione ed emissione dell'organigramma aziendale e degli ordini di servizio che ne elencano le principali responsabilità;
- individua processi di controllo e gestione delle risorse finanziarie, adeguati a prevenirne utilizzi inadeguati con riferimento particolare ai reati oggetto del Decreto Legislativo 231/01;
- attribuisce all' Organismo di Vigilanza il compito di vigilare sul funzionamento del Modello 231, sul controllo dell'osservanza e sulle opportunità di aggiornamento.

L'adozione del Modello 231 è, pertanto, finalizzata a:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- diffondere la consapevolezza che, dalla violazione del Decreto, delle prescrizioni contenute nel Modello e/o dei principi del Codice Etico possa derivare l'applicazione di misure sanzionatorie (pecuniarie e/o interdittive) anche a carico della Società ovvero gravi lesioni all'immagine ed alla reputazione del Gruppo;
- diffondere una cultura d'impresa improntata alla legalità, nella consapevolezza dell'espressa riprovazione da parte di Cy4gate di ogni comportamento contrario alla legge, ai regolamenti, alle disposizioni interne e, in particolare, alle disposizioni contenute nel presente Modello e nel Codice Etico;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di Cy4gate che la violazione delle prescrizioni contenute nel Modello 231 della Società può comportare l'applicazione di apposite sanzioni ivi inclusa la risoluzione del rapporto contrattuale;

- dare evidenza dell'esistenza di una struttura organizzativa efficace e coerente con il modello operativo adottato, con particolare riguardo alla chiara attribuzione dei poteri, alla formazione delle decisioni e alla loro trasparenza e motivazione, ai controlli sugli atti e le attività, nonché alla correttezza e veridicità dell'informativa interna ed esterna;
- consentire alla Società, grazie ad un sistema di presidi di controllo e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione dei reati rilevanti ai sensi del Decreto.

2.7 Identificazione analitica delle attività sensibili e delle aree critiche.

L' individuazione delle specifiche aree di attività della Società considerate a rischio in relazione alla problematica in oggetto, e quella dei singoli reati, tra quelli presi in considerazione, ipoteticamente collegabili alle stesse, è contenuta nelle Tabelle delle attività a rischio e dei relativi controlli.

Esse rappresentano il punto di partenza concettuale della realizzazione del sistema di gestione del rischio, posto che sulla base delle relative risultanze sono state identificate anche le misure interne preventive che il soggetto agente, se determinato a delinquere, deve necessariamente violare per originare la responsabilità amministrativa dell'ente.

La loro conoscenza preventiva costituisce elemento importante per qualunque soggetto che operi per la Società e la relativa lettura cognitiva è, quindi, strumento di base permanente per ogni possibile intervento preventivo di tutti gli organi interni.

La individuazione e descrizione delle attività a rischio si pone, poi, in diretta relazione con le diverse fattispecie di reato richiamate dal Decreto 231/2001 e prese in considerazione dal Modello, astrattamente, configurabili con riferimento alle medesime attività.

Pertanto, la connessione tra l'attività posta in essere, da un lato, e la fattispecie di reato presupposto dall'altro lato, è stata identificata tramite il fattore della potenzialità astratta riferita a possibili comportamenti deviati del singolo operatore di cui si sottolinea, volta per volta, l'effettuabilità teorica anche in ragione dell'assenza di verifiche o di riscontri contemporanei di soggetti terzi in qualunque modo presenti alle operazioni.

2.8 Destinatari

Si considerano soggetti destinatari delle prescrizioni del Modello (di seguito, i "Destinatari"), ai sensi del Decreto e nell'ambito delle rispettive competenze, i componenti degli organi sociali, il management e i dipendenti di Cy4gate, nonché tutti coloro che, a diverso titolo, collaborano e/od operano per il conseguimento dello scopo e degli obiettivi della Società (es. collaboratori, partner, fornitori, etc.).

2.9 Struttura del Modello

Il presente Modello è costituito da una Parte Generale composta da quattro sezioni che contengono, nell'ordine:

- una sintetica descrizione del quadro normativo, integrata dal dettaglio delle fattispecie di reato;

- la descrizione del Modello 231 e delle sue componenti essenziali ivi incluse le regole che disciplinano le modalità di diffusione ed aggiornamento del Modello;
- le regole riguardanti la costituzione dell'Organismo di Vigilanza;
- le sanzioni applicabili in caso di violazioni delle regole e delle prescrizioni contenute nel Modello;

e da Parti Speciali che contengono una descrizione relativa:

- alle diverse fattispecie di reato-presupposto concretamente e potenzialmente rilevanti in azienda, individuate in ragione delle caratteristiche peculiari dell'attività svolta da Cy4gate;
- alle attività a rischio-reato;
- alle regole comportamentali, ai principi di controllo specifici e ai presidi organizzativi.

2.10 Presupposti del Modello

Nella predisposizione del Modello, Cy4gate ha tenuto conto del proprio sistema di controllo interno, gestito anche attraverso il Sistema di Qualità Aziendale, e quello relativo alla Sicurezza e Sanità dei Lavoratori (ex D.lgs. 81/2008), al fine di verificare la capacità di prevenire le fattispecie di reato previste dal Decreto nelle attività identificate a rischio, nonché dei principi etico – sociali, ai quali si attiene nello svolgimento delle proprie attività.

Più in generale, il sistema di controllo interno di Cy4gate è orientato a garantire, con ragionevole certezza, il raggiungimento di obiettivi operativi, di informazione e di conformità ed, in particolare:

- l'obiettivo operativo del sistema di controllo interno riguarda l'efficacia e l'efficienza della Società nell'impiegare le risorse,

nel proteggersi dalle perdite, nel salvaguardare il patrimonio aziendale. Tale sistema è volto, inoltre, ad assicurare che il personale operi per il perseguimento degli obiettivi aziendali;

- l'obiettivo di informazione si traduce nella predisposizione di rapporti tempestivi ed affidabili per il processo decisionale sia interno che esterno all'organizzazione aziendale;
- l'obiettivo di conformità garantisce, invece, che tutte le operazioni ed azioni siano condotte nel rispetto delle leggi e dei regolamenti, dei requisiti prudenziali e delle procedure aziendali interne.

Il sistema di controllo interno di Cy4gate si basa sui seguenti elementi:

- integrità e valori che ispirano l'agire quotidiano dell'intera Società;
- sistema organizzativo formalizzato e chiaro nell'attribuzione dei poteri e delle responsabilità in coerenza con il raggiungimento degli obiettivi assegnati;
- attenzione al sistema delle competenze del personale, alla luce degli obiettivi perseguiti;
- identificazione, valutazione e gestione dei rischi che potrebbero compromettere il raggiungimento degli obiettivi aziendali;
- definizione di procedure aziendali, parte del complessivo sistema normativo della Società, che esplicitano i controlli posti a presidio dei rischi e del raggiungimento degli obiettivi prefissati;
- sistemi informativi idonei a supportare i processi aziendali e il complessivo sistema di controllo interno (informatici, di reporting, ecc.);
- processi di comunicazione interna e formazione del personale;

- sistemi di monitoraggio a integrazione dei controlli di linea;
- audit interni periodici effettuati dal gruppo di audit di qualità e/o verifiche dirette o altri audit, la cui periodicità viene definita dall'O.d.V.

Tutti i Destinatari, nell'ambito delle funzioni svolte, sono responsabili della definizione e del corretto funzionamento del sistema di controllo attraverso i controlli di linea, costituiti dall'insieme delle attività di controllo che i singoli uffici svolgono sui loro processi.

2.11 Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali sviluppati dalla Cy4gate nella definizione del Modello, possono essere cosi riassunti:

- individuazione delle attività aziendali nel cui ambito è ipotizzabile la commissione di reati presupposto della responsabilità degli enti ai sensi del D.lgs. 231/2001 ("attività a rischio" o "attività sensibili"), svolta mediante l'analisi dei processi aziendali e delle possibili modalità realizzative delle fattispecie di reato;
- predisposizione e aggiornamento di strumenti normativi relativi ai processi ritenuti a rischio potenziale di commissione di reato, diretti a regolamentare espressamente la formazione e l'attuazione delle decisioni della Società, al fine di fornire indicazioni puntuali sul sistema dei controlli preventivi in relazione alle singole fattispecie di illecito da prevenire;
- gestione dei processi aziendali secondo gli standard ISO certificabili, caratterizzata da un proprio sistema di controllo particolarmente rigoroso;

- adozione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste, sancite nel Codice Etico della Cy4gate e, più in dettaglio, nel presente Modello;
- istituzione di un Organismo di Vigilanza al quale sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello ai sensi dell'art. 6, punto b), del Decreto;
- attuazione di un sistema sanzionatorio idoneo a garantire l'effettività del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione, sensibilizzazione, divulgazione e formazione sui contenuti del Modello, nonché sulle regole comportamentali valide a tutti i livelli aziendali, caratterizzata da capillarità, obbligatorietà di partecipazione, verifica dell'apprendimento e costante aggiornamento;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso;
- individuazione delle attività "a rischio".

L'art. 6, comma 2, lett. a) del Decreto prevede, espressamente, che il Modello dell'ente individui le attività aziendali nel cui ambito possano essere, potenzialmente, commessi i reati di cui al medesimo Decreto.

In relazione alle singole fattispecie di reato previste dal D. Lgs. 231/01 è effettuata l'analisi del contesto aziendale per evidenziare dove, e secondo quali modalità, possono potenzialmente verificarsi eventi pregiudizievoli per gli obiettivi indicati dal citato decreto.

Tale analisi dei rischi, comprensiva dei processi e delle attività sensibili rilevanti, direttamente o indirettamente riferibili al rischio

di reato, è eseguita dalla competente funzione aziendale, che la sottopone dapprima all'Organismo di Vigilanza della società per le eventuali proposte di integrazioni, e successivamente all'Amministratore Delegato per l'effettivo recepimento. Tale analisi costituisce la base di riferimento per eventuali esigenze di modifica e/o di integrazione del Modello.

A ciascuna attività sensibile è associata l'indicazione della Funzione aziendale responsabile, nonché delle modalità di possibile realizzazione dei reati.

La mappatura degli ambiti operativi di potenziale esposizione della Società ai diversi rischi - reato 231 è accompagnata dalla rilevazione degli specifici elementi di controllo esistenti, nonché dalla definizione di eventuali iniziative di integrazione e/o rafforzamento dei presidi in essere.

In base alle indicazioni e alle risultanze della complessiva attività di analisi sopra delineata, le singole Funzioni aziendali implementano - previa valutazione dei rischi individuati e definizione delle politiche di gestione degli stessi - le norme interne e gli strumenti normativi ed organizzativi che governano i processi afferenti le attività a rischio (es. procedure, policy, linee guida).

2.12 Principi e presìdi generali di controllo interno

Per tutte le attività a rischio descritte nelle singole parti speciali, valgono i seguenti principi di controllo generali:

- esplicita formalizzazione delle norme comportamentali;
- chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna Funzione ed alle diverse qualifiche e ruoli professionali;

- precisa descrizione delle attività di controllo e loro tracciabilità;
- adeguata segregazione di ruoli operativi e ruoli di controllo;
- sistemi informativi integrati e orientati, oltre alla segregazione delle funzioni, anche 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.

In particolare, devono essere perseguiti i seguenti presìdi organizzativo-gestionali di carattere generale.

Norme comportamentali.

Adozione ed adesione al Codice Etico nel quale sono indicate le regole generali di condotta a presidio delle attività svolte.

Definizioni di ruoli e responsabilità.

La regolamentazione interna deve declinare ruoli e responsabilità delle strutture organizzative a tutti i livelli, descrivendo in maniera omogenea le attività proprie di ciascuna struttura.

Tale regolamentazione deve essere resa disponibile e conosciuta all'interno dell'organizzazione.

Protocolli e norme interne.

Le attività sensibili devono essere regolamentate, in modo coerente e congruo, attraverso gli strumenti normativi aziendali, così che in ogni momento si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato.

Segregazione dei compiti

All'interno di ogni processo aziendale sensibile, devono essere separate le funzioni o i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla.

Non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise, e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno.

Poteri autorizzativi e di firma

Deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando l'impresa e manifestando la sua volontà.

I poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate.

Le procure devono essere coerenti con il sistema interno delle deleghe.

Devono essere previsti meccanismi di pubblicità delle procure assegnate ai primi livelli verso gli interlocutori esterni.

Devono essere previsti meccanismi di rendicontazione dei poteri delegati e delle relative procure.

Devono essere previste modalità di revoca delle procure e delle deleghe assegnate.

Il processo di attribuzione delle deleghe deve identificare, tra l'altro:

- la posizione organizzativa che il delegato ricopre in ragione dello specifico ambito di operatività della delega;

- l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguente assunzione degli obblighi conferiti;
- i limiti di spesa attribuiti al delegato.

Le deleghe devono essere attribuite secondo i principi di:

- autonomia decisionale e finanziaria del delegato;
- idoneità tecnico-professionale del delegato;
- disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni;
- attività di controllo e tracciabilità.

La società è dotata della Information Security Policy. In tale documento sono definiti ruoli e responsabilità per quanto riguarda i processi che concorrono alla definizione, al mantenimento ed alla verifica del Sistema di gestione della Sicurezza delle Informazioni, ovvero l'insieme delle politiche che consentono di gestire la sicurezza delle informazioni.

La Società è dotata di un sistema di controllo di accesso centralizzato. L'accesso avviene tramite *badge* sia per il personale dipendente sia per i lavoratori interinali che per i visitatori. La figura dell'IT manager verifica, periodicamente, l'efficacia dei controlli di accesso fisico alle aree sia durante il normale orario di lavoro che in altri orari.

La Società è dotata della procedura di Gestione dei servizi IT. Tale procedura definisce le modalità di gestione e salvaguardia dell'infrastruttura IT necessaria per la corretta erogazione dei servizi informativi.

I servizi erogati dal sistema ICT sono:

- gestione delle email;
- gestione infrastruttura laboratorio;

- gestione file server;
- gestione source code repository;
- gestione trouble ticket management;
- gestione fonia mobile;
- gestione controlli accessi;
- gestione tool amministrazione;
- gestione backup;
- gestione connettività internet;
- gestione postazioni di lavoro.

I documenti riguardanti l'attività della Società ed, in particolare, i documenti o la documentazione informatica riguardanti attività sensibili, sono archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza.

L'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o ad un loro delegato, al Collegio Sindacale o a funzioni e organi deputati al controllo compreso l'Organismo di Vigilanza.

2.13 Codice di comportamento

Nel Codice Etico diffuso a tutti i dipendenti della Società sono fissati i principi guida e le direttive fondamentali, a cui devono conformarsi le attività ed i comportamenti delle persone alle quali il Codice stesso è destinato, incluse le regole di comportamento che i Fornitori e i Partner sono tenuti ad osservare specificamente nell'ambito delle attività oggetto di contratto, nonché il relativo sistema sanzionatorio in caso di violazione dello stesso.

Nel predetto Codice è descritto il relativo sistema sanzionatorio, applicabile in caso di violazione degli stessi.

Il Codice, pur essendo dotato di una propria valenza autonoma, integra il complessivo sistema di prevenzione degli illeciti di cui al D. Lgs. 231/2001 e costituisce un elemento fondamentale e portante del Modello stesso.

Tale Codice è altresì un riferimento per tutte le specifiche politiche e gli strumenti normativi che disciplinano le attività potenzialmente esposte ai rischi di reato.

2.14 Aggiornamento del Modello

La verifica sull'aggiornamento e sull'efficace attuazione del Modello compete al Consiglio di Amministrazione al quale, pertanto, è attribuito il potere di apportare modifiche al Modello, che lo eserciterà mediante delibera con le modalità previste per la sua adozione.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal D. Lgs. 231/2001.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione ovvero dell'Amministratore Delegato. L'Organismo di Vigilanza, nell'ambito dei poteri ad esso conferiti conformemente agli art. 6, comma 1 lett. b) e art. 7, comma 4 lett. a) del Decreto, ha la responsabilità di formulare proposte motivate,

in ordine all'aggiornamento e all'adeguamento del presente Modello sottoponendole all'approvazione del Consiglio di Amministrazione.

In ogni caso il Modello deve essere tempestivamente modificato ed integrato dal Consiglio di Amministrazione, anche su proposta e previa consultazione dell'Organismo di Vigilanza, quando siano intervenute:

- violazioni ed elusioni delle prescrizioni in esso contenute che ne abbiano evidenziato l'inefficacia o l'incoerenza ai fini della prevenzione dei reati;
- significative modificazioni all'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa;
- modifiche normative ed evoluzioni giurisprudenziali.

Le modifiche, gli aggiornamenti e le integrazioni del Modello devono essere sempre comunicati all'Organismo di Vigilanza.

2.15 Metodologia per l'implementazione del Modello e la valutazione del rischio.

La metodologia d'implementazione e aggiornamento del Modello Organizzativo segue la strutturazione in fasi sulla base della migliore prassi e delle indicazioni delle linee guida delle principali associazioni di categoria (il riferimento principale è rappresentato dalle linee guida di Confindustria), al fine di garantire la qualità e l'autorevolezza dei risultati.

Sulla base delle citate Linee Guida e del Codice Etico, le fasi di lavoro seguite sono:

• l'identificazione, tra i reati previsti dal catalogo "231" di quelli che possono ritenersi rischi inerenti e quelli non inerenti rispetto ai processi, alle attività ed in genere alle attività di business della

Società, distinguendo per i reati inerenti i comportamenti finali dalle condotte strumentali (es. rispetto delle regole contabili per evitare la generazione di provviste finalizzate ad attività corruttive);

• l'identificazione delle attività sensibili ("as-is analysis"). Tale fase è finalizzata all'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati richiamati dal d.lgs. 231/01 e delle attività strumentali alla commissione dei reati. L'identificazione del livello di rischio, viene eseguita sulla base di criteri quantitativi e qualitativi;

• l'effettuazione della *gap analysis*. L'attività di *gap analysis* è rivolta ad individuare sia i requisiti organizzativi che caratterizzano un Modello organizzativo idoneo a prevenire i reati richiamati dal d.lgs. 231/2001, sia le azioni di miglioramento del rispetto ai controlli preesistenti mediante un'analisi comparativa i presidi di controllo.

SEZIONE TERZA

ORGANISMO DI VIGILANZA

PREMESSA

L'art. 6 del Decreto prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi.

L'Organismo di Vigilanza di Cy4gate è composto da componenti di comprovata esperienza e competenza, con requisiti di onorabilità, professionalità ed indipendenza.

Essi sono nominati dal Consiglio di Amministrazione che ne determina anche la remunerazione.

L'Organismo di Vigilanza dura in carica tre anni e, comunque, fino alla data dell'Assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della carica.

Può essere individuato componente dell'O.d.V. uno dei responsabili delle funzioni a cui non siano conferiti ruoli gestionali o, comunque, operativi e che presenti adeguati requisiti di indipendenza, professionalità e onorabilità.

In ogni caso, alla scadenza del mandato, ciascun componente dell'Organismo di Vigilanza rimane in carica sino alla nomina del nuovo Organismo di Vigilanza da parte del Consiglio di Amministrazione.

Sono, comunque, fatti salvi i casi di dimissioni di un membro dell'Organismo di Vigilanza che hanno efficacia immediata.

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e controllo e di un proprio regolamento interno.

L'Organismo esercita tutti i poteri di sorveglianza, anche preventiva, relativi alle procedure operative e di controllo interne, ed ai protocolli istituiti in osservanza del comma 2 dell'art. 6 del Decreto 231/2001 e in materia di antiriciclaggio (ove applicabile), in applicazione dei quali può richiedere anche assistenza interna all'ente attraverso i responsabili di ogni singola funzione interessata.

Per l'esercizio dei poteri di sorveglianza sulle attività sociali l'Organismo può incaricare terzi di condurre indagini o verifiche anche sui registri o altri atti dell'Ente.

Il Decreto enuncia (art. 6 comma 2 lettera d.), tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza.

Regolamento costitutivo e di funzionamento dell'Organismo di Vigilanza

L'Organismo di Vigilanza opera in conformità alle prescrizioni di seguito formulate.

Art. 1

Organismo di Vigilanza

È Organismo di Vigilanza (di seguito, Organismo) di Cy4gate l'organismo di nomina direzionale costituito, ai sensi dell'art. 6 comma 1, lett. b), del Decreto Legislativo 8 giugno 2001 n. 231,

all'interno dell'Ente, dotato di autonomi poteri di iniziativa e controllo riferiti all'applicazione delle norme del citato decreto, al Modello ed alle procedure aziendali ivi contenute e/o richiamate. La funzionalità operativa dell'Organismo è assicurata dall'applicazione obbligatoria del presente regolamento.

Art. 2

Nomina e composizione dell'Organismo di Vigilanza

L'Organismo è composto da un numero di tre membri nominati dal Consiglio di Amministrazione della medesima Società per un periodo di durata di tre esercizi.

Possono far parte dell'Organismo persone dotate di valida e riconosciuta esperienza in tematiche giuridiche, economiche o gestionali d'azienda, purché nel loro insieme garantiscano al medesimo Organismo caratteristiche di autonomia, indipendenza, professionalità e continuità di azione.

Il Consiglio di Amministrazione, all'atto della nomina, designa anche il Presidente dell'Organismo. Nessun dipendente o soggetto interno può essere nominato quale Presidente dell'Organismo.

Art. 3

Cause di ineleggibilità, decadenza e revoca

Costituiscono cause di ineleggibilità e/o decadenza dei componenti dell'O.d.V.:

- aver ricoperto funzioni di amministratore esecutivo, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;

- aver riportato una sentenza di condanna passata in giudicato, anche conseguente a richiesta di applicazione della pena (cosiddetto "patteggiamento"), in Italia o all'estero, in relazione a reati della stessa indole di quelli previsti dal Decreto;
- aver riportato una condanna con sentenza passata in giudicato, ad una pena che importa l'interdizione anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
- mancata partecipazione ad almeno tre riunioni consecutive senza giustificato motivo;
- venir meno, nel corso del periodo di carica triennale, dei requisiti che hanno determinato l'individuazione dei componenti stessi all'atto delle nomine e, in virtù della carica societaria o del ruolo organizzativo rivestito.

Costituiscono cause di revoca dei componenti dell'O.d.V.:

- l'omessa e/o insufficiente vigilanza da parte dell'O.d.V. risultante da una sentenza di condanna passata in giudicato, emessa nei confronti della Società ai sensi del Decreto 231, anche a seguito di richiesta di applicazione della pena (patteggiamento);
- il grave inadempimento delle funzioni e/o doveri dell'Organismo di Vigilanza.

La revoca è disposta con delibera del Consiglio di Amministrazione approvata con il voto dei due terzi dei presenti e sentiti gli altri membri dell'O.d.V. ed il Collegio Sindacale.

In caso di decadenza o revoca di uno dei componenti dell'O.d.V., il Consiglio di Amministrazione provvede, tempestivamente, alla sua sostituzione.

La revoca di uno o di tutti i membri dell'Organismo può essere disposta, esclusivamente, con deliberazione del Consiglio di Amministrazione assunta con il voto favorevole di tanti amministratori che rappresentino almeno i 2/3 dell'intero Consiglio. I membri dell'Organismo possono essere revocati, oltre che per i casi sopra indicati, per quelli tassativamente indicati nella delibera dell'organo amministrativo di nomina e conferimento dell'incarico.

Se durante il corso dei tre esercizi uno o due membri dell'Organismo dovessero rinunciare alla carica o venire, comunque, meno rispetto alla funzione, il Consiglio può sostituirli con altri membri di pari funzione (purché nel rispetto di quanto previsto dal presente articolo), fino alla scadenza naturale del periodo di nomina dell'Organismo.

Anche prima del passaggio in giudicato della sentenza, il Consiglio di Amministrazione di Cy4gate, qualora un componente dell'Organismo di Vigilanza sia stato condannato in primo grado per delitti di particolare gravità, e/o nel caso in cui sia stata disposta nei suoi confronti una misura cautelare personale, potrà optare per la revoca o la sospensione dei poteri del singolo membro e la eventuale nomina di un soggetto *ad interim*.

Art. 4

Compiti e poteri dell'Organismo di Vigilanza

Costituiscono compiti istituzionali dell'Organismo:

- la vigilanza sul funzionamento del Modello istituito ai sensi del Decreto 231/2001;
- la vigilanza sull'osservanza, interna ed esterna all'ente, del Modello;
- la redazione di periodici aggiornamenti del Modello;

- la vigilanza sull'osservanza delle norme (ove applicabili) previste in materia di antiriciclaggio.

In aggiunta ai compiti attribuiti ai sensi del Decreto 231/2001 come sopra indicati, all'Organismo di Vigilanza è attribuito, altresì, il compito di monitorare, direttamente o indirettamente, il rispetto, da parte del personale preposto, delle procedure operative interne e delle normative applicabili.

Il Consiglio di Amministrazione mette a disposizione, su richiesta ed a seconda delle necessità espresse dall'O.d.V., adeguate risorse aziendali in relazione ai compiti affidatigli e, nel predisporre il budget aziendale, approva - sulla base di quanto proposto dall'Organismo di Vigilanza stesso - una dotazione adeguata di risorse finanziarie della quale l'O.d.V. potrà disporre per il corretto svolgimento dei propri compiti.

L'Organismo è, altresì, tenuto a comunicare formalmente il Modello della Società a ciascun componente degli organi sociali direttivi e di controllo.

In relazione alle attività sensibili, l'O.d.V. predispone ed esegue un piano di attività e verifiche finalizzate a valutare, monitorare e vigilare sull'effettiva applicazione, l'adeguatezza e la funzionalità degli strumenti normativi, in termini di presìdi atti a prevenire la commissione dei reati previsti dall'impianto normativo.

L'Organismo istituisce un piano di comunicazione reciproca con gli organi sociali e con tutti i soggetti, interni o esterni incaricati dello svolgimento di attività di controllo interno. L'Organismo ha, altresì, il potere di consultazione di tutti i libri e registri dell'ente istituiti in applicazione di qualsivoglia norma di legge.

Tenuto conto della peculiarità delle attribuzioni dell'Organismo e dei contenuti professionali, lo stesso potrà avvalersi nell'ambito delle disponibilità previste ed approvate da apposito *budget*, della

collaborazione di altre funzioni di direzione e controllo dell'ente che di volta in volta si rendessero necessarie, nonché di professionisti e consulenti esterni.

Con riferimento ai predetti poteri di sorveglianza l'Organismo - tenuto conto della particolare struttura del Modello di Cy4gate quale documento anche di raccordo ed integrazione dei sistemi di *compliance* aziendale già in vigore presso la Società – potrà esercitare parte degli stessi anche richiedendo, come organo referente, l'ausilio dei soggetti responsabili dei sistemi di controllo già adottati dalla Società, al fine di coordinare e massimizzare le attività già svolte da questi ultimi, eventualmente, anche predisponendo apposite "*check list*" da utilizzare nello svolgimento delle rispettive citate attività di controllo.

A tal fine, l'Organismo potrà periodicamente organizzare incontri individuali o collettivi con i diversi responsabili preposti alle diverse funzioni di controllo, al fine di recepire da questi i resoconti delle rispettive attività di controllo ed, in particolare, le loro segnalazioni in ordine ad eventuali anomalie e criticità, nonché eventuali suggerimenti su possibili modifiche del Modello. All'esito della predetta attività di affiancamento e di coordinamento dei soggetti responsabili delle diverse funzioni di controllo citate, potranno essere valutate eventuali ulteriori misure organizzative da modificare e/o adottare.

L'Organismo può ascoltare il Presidente, l'Amministratore Delegato o altro consigliere (ognuno individualmente).

In alternativa a quanto precede, l'Organismo può procedere ad assumere le predette informazioni anche tramite idonea reportistica scritta consegnata, debitamente firmata da parte del soggetto che rilascia le informazioni medesime.

Art. 5

Reporting dell'Organismo di Vigilanza nei confronti degli Organi Societari

L'O.d.V. relaziona in merito alle attività di propria competenza nei confronti del Consiglio di Amministrazione e del Collegio Sindacale, in particolare:

- su base continuativa, direttamente nei confronti del Presidente del Consiglio di Amministrazione e/o dell'Amministratore Delegato, anche mediante l'invio delle verbalizzazioni delle proprie riunioni o di loro estratti, aventi ad oggetto l'attività complessivamente svolta, le criticità emerse, l'analisi delle segnalazioni e delle relative iniziative assunte, le proposte di revisione e aggiornamento del Modello, l'informazione sul Piano di attività per l'anno successivo;
- su base periodica, almeno annuale, nei confronti del Consiglio di Amministrazione e/o dell'Amministratore Delegato e del Collegio Sindacale, mediante una relazione relativa all'attuazione del Modello da parte della Società, le sue eventuali carenze, nonché su elementi rilevanti e di carattere generale in merito all'adozione del Modello Organizzativo. Attraverso tale relazione l'Organismo provvede anche a riferire e/o riepilogare eventuali disapplicazioni e violazioni del Modello, indicando tutte le opportune azioni correttive da intraprendere. Le eventuali violazioni reiterate e di particolare gravità dovranno essere comunicate tempestivamente al Presidente ed all'Amministratore Delegato, al Consiglio di Amministrazione ed al Collegio Sindacale;
- informa con tempestività il C.d.A. ogni qualvolta riscontri situazioni di particolare gravità.

L'O.d.V. può essere convocato in qualsiasi momento dal Consiglio di Amministrazione o dal Collegio Sindacale per riferire in merito al funzionamento e all'osservanza del Modello o a situazioni specifiche.

Art. 6

Flussi informativi nei confronti dell'Organismo di Vigilanza

Al fine di soddisfare le esigenze enunciate nel Decreto (art. 6 comma 2 lettera d) sono istituiti specifici obblighi informativi nei confronti dell'Organismo di Vigilanza.

A tal fine, sono previsti:

- flussi informativi periodici, quali ad esempio:
  - quelli relativi alle variazioni procedurali significative ai fini del Modello 231;
  - l'informativa periodica sulle attività a rischio di maggior rilievo e sullo stato di predisposizione e aggiornamento degli strumenti normativi interni;
  - le eventuali comunicazioni della società di revisione;
  - i bilanci e le relazioni;
- flussi informativi *ad hoc*, attinenti a:
  - criticità attuali o potenziali che, a titolo esemplificativo, possono emergere da notizie occasionali provenienti dalla struttura o dagli organi sociali attinenti ad attività di *business*; variazioni organizzative significative ai fini del Modello 231;
  - aggiornamenti del sistema dei poteri;
  - notizie relative a procedimenti o indagini aventi ad oggetto reati previsti dal Decreto 231;

– procedimenti disciplinari a carico dei Destinatari per violazione del Modello 231 o del Codice Etico.

Tra i flussi informativi che devono essere, obbligatoriamente, e tempestivamente trasmessi all'Organismo di Vigilanza, rientrano le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, tributaria o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento della Società o di soggetti apicali, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;
- richieste di informazioni o invio di prescrizioni, relazioni ed ogni altra documentazione che scaturisce da attività di ispezione delle stesse svolte e rientranti negli ambiti di pertinenza del D.Lgs. 231/2001;
- comunicazioni all'Autorità Giudiziaria che riguardano potenziali o effettivi eventi illeciti che possono essere riferiti alle ipotesi di cui al D.Lgs. 231/2001;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- esiti delle attività di controllo svolte dai responsabili delle diverse funzioni aziendali dalle quali siano emersi fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o del Modello;
- modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza dei procedimenti disciplinari svolti e

delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;

- segnalazione di infortuni gravi (incidenti mortali o con prognosi superiore a 40 giorni) occorsi a dipendenti, appaltatori e/o collaboratori presenti nei luoghi di lavoro della Società;
- relazione degli audit interni di riscontro eseguiti nell'ambito di quanto definito nel sistema della Qualità, nel Sistema di Risk Management e di controllo, realizzati secondo il programma definito dell'O.d.V..

Art. 7

Procedura di segnalazione all'Organismo di Vigilanza

Il personale dipendente, a tutela dell'integrità della Società, è tenuto a trasmettere segnalazioni circostanziate di condotte illecite rilevanti, ai sensi del Decreto 231 e fondate su elementi di fatto precisi e concordanti, o di violazioni del presente Modello Organizzativo, di cui sia venuto a conoscenza in ragione delle funzioni svolte, mediante i seguenti canali di comunicazione:

- posta elettronica: odv231@cy4gate.com disponibile anche nella rubrica aziendale;
- posta tradizionale: via Morolo 92, 00131 Roma, Italy.

Nelle attività di gestione delle segnalazioni è garantita la riservatezza dell'identità del segnalante.

La Società, inoltre, garantisce il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

In ogni caso, qualora l'O.d.V. ritenga di procedere ad un ulteriore accertamento dei fatti, può avvalersi del supporto delle funzioni aziendali di controllo.

Tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite dall'Organismo di Vigilanza per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o, successivamente, trattati e, comunque, nel rispetto delle policy e delle procedure interne in tema di trattamento dei dati personali.

(a) Segnalazioni vietate.

Le segnalazioni devono sempre avere un contenuto da cui emerga un leale spirito di partecipazione al controllo e alla prevenzione di fatti nocivi degli interessi generali, e non possono in alcun modo essere lo strumento per dar sfogo a dissapori o contrasti tra dipendenti.

È parimenti vietato:

- il ricorso ad espressioni ingiuriose;
- l'inoltro di segnalazioni con finalità puramente diffamatorie o calunniose;
- l'inoltro di segnalazioni che attengano esclusivamente ad aspetti della vita privata, senza alcun collegamento diretto o indiretto con l'attività aziendale. Tali segnalazioni saranno ritenute ancor più gravi quando riferite ad abitudini e orientamenti sessuali, religiosi, politici e filosofici.

(b) Contenuto delle segnalazioni.

Il segnalante è tenuto a fornire tutti gli elementi a lui noti, utili a riscontrare, con le dovute verifiche, i fatti riportati.

In particolare, la segnalazione deve contenere i seguenti elementi essenziali:

- Le generalità del segnalante;
- L'oggetto. È necessaria una chiara descrizione dei fatti oggetto di segnalazione, con indicazione (se conosciute) delle circostanze di tempo e luogo in cui sono stati commessi/omessi i fatti.
- Il segnalato. Il segnalante deve indicare le generalità o, comunque, altri elementi (come la funzione/ruolo aziendale) che consentano un'agevole identificazione del presunto autore del comportamento illecito.

Inoltre, il segnalante potrà indicare i seguenti ulteriori elementi:

- l'indicazione di eventuali altri soggetti che possono riferire sui fatti narrati;
- l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
- ogni altra informazione che possa agevolare la raccolta di evidenze su quanto segnalato.

Art. 8

Adunanze

L'Organismo si riunisce con cadenza trimestrale, ovvero su richiesta del Consiglio d'Amministrazione in ragione di qualsivoglia necessità operativa connessa alle norme del Decreto 231/2001, ovvero in ogni caso quando ritenuto opportuno.

La convocazione dell'Organismo è disposta dal Presidente con mezzi adeguati a garantirne la conoscenza almeno 5 (cinque) giorni prima della prevista adunanza. La convocazione dell'Organismo non è

ritenuta necessaria qualora siano presenti tutti i componenti dello stesso.

Le adunanze dell'Organismo sono presiedute dal Presidente o, in sua assenza, dal componente più anziano di età. In nessun caso può assumere la presidenza dell'adunanza un dipendente o, comunque, un soggetto interno.

Le adunanze dell'Organismo sono ritenute valide con la presenza della maggioranza dei suoi componenti. Le deliberazioni sono assunte con la maggioranza dei componenti presenti. In caso di parità di voto prevale il voto del Presidente.

Prima dell'avvio di ogni riunione, l'Organismo provvede a nominare, tra i suoi componenti, un segretario con funzioni di verbalizzazione.

Il verbale delle adunanze, redatto dal segretario e sottoscritto da quest'ultimo unitamente al Presidente, viene conservato in un apposito registro.

Art. 9

Riservatezza e segretezza

L'Organismo si impegna a garantire che qualsiasi informazione, dato, notizia, relativi alla Cy4gate dovesse conoscere ed acquisire nel corso dello svolgimento del proprio incarico sarà: (i) ritenuto e mantenuto confidenziale; (ii) utilizzato, esclusivamente, per l'esecuzione dell'incarico stesso; (iii) conservato per un tempo limitato e, comunque, strettamente necessario al soddisfacimento della finalità al quale è preordinato.

Art. 10

Archiviazione

Tutte le risultanze delle verifiche effettuate dall'Organismo debbono essere formalizzate in documenti conservati, unitamente ai verbali delle adunanze, in apposito archivio cartaceo o elettronico.

Le modalità di conservazione di tale documentazione sono rimesse alla discrezionalità dell'Organismo, purché ne sia comunque garantita la riservatezza, l'integrità e la pronta disponibilità.

Copia della documentazione necessaria per l'attività di verifica è conservata in appositi archivi ad accesso limitato.

Art. 11

Rinvio

Per quanto non espressamente previsto dal presente regolamento, si fa rinvio e riferimento a quanto contenuto nel Modello.

In caso di contrasto tra il presente regolamento ed il Modello, sarà quest'ultimo a prevalere.

SEZIONE QUARTA

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

4.1 Formazione del personale

Cy4gate promuove la conoscenza del Modello e dei relativi aggiornamenti tra tutti i dipendenti, che sono pertanto tenuti a conoscerlo e ad attuarlo.

L' Unità Organizzativa *Human Resources* gestisce la formazione del personale sui contenuti del Decreto e sull'attuazione del Modello, dandone evidenza all' OdV.

In tale contesto, le azioni comunicative prevedono:

- l'inserimento del Modello, del Codice Etico nell'*intranet* aziendale;
- la messa a disposizione del Codice Etico per tutto il personale in forza, nonché la distribuzione di tali documenti ai nuovi assunti al momento dell'inserimento in azienda, con firma attestante l'avvenuta ricezione e l'impegno alla conoscenza e al rispetto delle relative prescrizioni;
- l'aggiornamento sulle modifiche apportate al Modello ed al Codice Etico.

Il percorso di formazione è articolato sui livelli qui di seguito indicati:

- personale direttivo e con funzioni di rappresentanza: incontri con i Responsabili di primo livello e "*workshop*" in aula con i dirigenti;
- altro personale: informativa in sede di assunzione; corso di formazione realizzato mediante incontri o con modalità *"e-learning"* attraverso supporto informatico presso l'*intranet* aziendale.

Eventuali sessioni formative di aggiornamento saranno effettuate, in caso di rilevanti modifiche apportate al Modello, ove l'OdV non ritenga sufficiente, in ragione della complessità della tematica, la semplice diffusione della modifica con le modalità sopra descritte.

4.2 Informativa a Collaboratori Esterni, Consulenti e Partner

Cy4gate promuove la conoscenza e l'osservanza del Modello, del Codice Etico anche tra i *partner* commerciali e finanziari, i consulenti, i collaboratori a vario titolo ed i fornitori della Società.

SEZIONE QUINTA

SISTEMA SANZIONATORIO

PREMESSA

La definizione di un sistema sanzionatorio, applicabile in caso di violazione delle disposizioni del presente Modello, costituisce condizione necessaria per garantire l'efficace attuazione del Modello stesso, nonché presupposto imprescindibile per consentire alla Società di beneficiare dell'esimente dalla responsabilità amministrativa (ex art. 6, comma 2, lettera e) del Decreto).

L'applicazione delle sanzioni disciplinari prescinde dall'instaurazione e dagli esiti di un procedimento penale, eventualmente, avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del D.Lgs. 231/2001.

Inoltre l'osservanza delle prescrizioni contenute nel Modello integra il comportamento che il dipendente è tenuto ad osservare anche in conformità alle regole di ordinaria diligenza e fedeltà disciplinate dagli artt. 2104 e 2105 c.c. per i dipendenti, ed è elemento essenziale del rapporto fiduciario e del corretto adempimento delle obbligazioni di Sindaci e Amministratori.

Le sanzioni comminabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché del rilievo e gravità della violazione commessa e del ruolo e responsabilità dell'autore. Più in particolare, le sanzioni comminabili sono diversificate tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di

eventuale recidiva, nonché dell'attività lavorativa svolta dall'interessato e della relativa posizione funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.

In generale, le violazioni possono essere ricondotte ai seguenti comportamenti:

- comportamenti che integrano una mancata attuazione colposa delle prescrizioni del Modello della Società e/o del Codice Etico;
- comportamenti che integrano una trasgressione dolosa delle prescrizioni del Modello e/o del Codice Etico, tale da compromettere il rapporto di fiducia tra l'autore e la Società in quanto preordinata in modo univoco a commettere un reato;

nonché classificate come segue:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, delle previsioni del Modello o delle procedure stabilite per l'attuazione del medesimo e del Codice Etico;
- la redazione, eventualmente in concorso con altri, di documentazione alterata o non veritiera;
- l'agevolazione, mediante condotta omissiva, di violazioni del Modello e del Codice Etico e della redazione da parte di altri, di documentazione alterata o non veritiera;
- l'omessa redazione della documentazione prevista dal Modello o dalle procedure stabilite per l'attuazione dello stesso.

Ai sensi e per gli effetti dell'art. 6 comma 2 *bis* del D. Lgs. 231/2001, introdotto dalla Legge 179/2017, la Società adotta sanzioni nei confronti dei soggetti che pongano in essere violazioni delle misure poste a tutela dei soggetti che segnalino la commissione di condotte illecite, rilevanti ai sensi del predetto decreto legislativo, ovvero che segnalino comportamenti posti in violazione del presente Modello.

La Società adotta, altresì, sanzioni nei confronti dei soggetti che effettuino con dolo o colpa grave segnalazioni di condotte illecite o di violazione del Modello, che si rivelino infondate.

Il procedimento sanzionatorio è, in ogni caso, gestito dalla funzione e/o dagli organi societari competenti che riferiscono al riguardo all'O.d.V.

Di seguito si riportano le sanzioni divise per tipologia di rapporto tra il soggetto e la Società.

5.1 Sanzioni per i lavoratori dipendenti

In relazione al personale dipendente, la Società si attiene alle prescrizioni di cui all'art. 7 della Legge 300/1970 (Statuto dei lavoratori) ed alle previsioni contenute nel Contratto Collettivo Nazionale di Lavoro applicabile, sia con riguardo alle sanzioni comminabili che alle modalità di esercizio del potere disciplinare.

L'inosservanza - da parte del personale dipendente - delle disposizioni del Modello e/o del Codice Etico, nonché di tutta la documentazione che di essi forma parte, costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro ex art. 2104 cod. civ. ed illecito disciplinare.

Più in particolare, l'adozione, da parte di un dipendente della Società, di un comportamento qualificabile, in base a quanto indicato al comma precedente, come illecito disciplinare, costituisce inoltre violazione dell'obbligo del lavoratore di eseguire con la massima diligenza i compiti allo stesso affidati, attenendosi alle direttive della Società, così come previsto dal vigente CCNL applicabile.

Alla notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. In particolare, nella fase di accertamento verrà previamente contestato al dipendente l'addebito e gli

sarà, altresì, garantito un congruo termine di replica. Una volta accertata la violazione, sarà irrogata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa.

Al personale dipendente possono essere comminate le sanzioni previste dal CCNL applicabile, che a titolo esemplificativo sono di seguito riportate:

- ammonizione inflitta verbalmente per le mancanze lievi;
- ammonizione scritta nei casi di recidiva delle infrazioni di cui al precedente punto;
- multa in misura non eccedente l'importo di 4 ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di giorni 10;
- licenziamento disciplinare senza preavviso e con le altre conseguenze di ragione e di legge.

Al fine di evidenziare i criteri di correlazione tra le violazioni e i provvedimenti disciplinari si precisa che:

- incorre nei provvedimenti disciplinari conservativi il dipendente che violi le disposizioni contenute nel Modello e in tutta la documentazione che di esso forma parte, o adotti, nello svolgimento di attività a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello stesso, dovendosi ravvisare in tale comportamento una mancata esecuzione degli ordini impartiti dalla Società;
- incorre, invece, nei provvedimenti disciplinari risolutivi il dipendente che:
  - adotti, nello svolgimento delle attività a rischio, un comportamento non conforme alle disposizioni contenute nel Modello, e nella documentazione che di esso forma parte, dovendosi ravvisare in tale comportamento una mancanza di

disciplina e di diligenza nel compimento dei propri obblighi contrattuali talmente grave da ledere la fiducia della Società nei confronti del dipendente stesso;

- adotti, nello svolgimento delle attività a rischio, un comportamento che si ponga palesemente in contrasto con le disposizioni contenute nel Modello e nella documentazione che di esso forma parte, tale da determinare la concreta applicazione a carico della Società delle misure previste dal D.Lgs. 231/2001, costituendo tale comportamento un atto che provoca alla Società grave nocumento morale e materiale e che non consente la prosecuzione del rapporto, neppure in via temporanea.

La Società non potrà adottare alcun provvedimento disciplinare nei confronti del dipendente senza il rispetto delle procedure previste nel CCNL applicabile per le singole fattispecie.

I principi di correlazione e proporzionalità tra la violazione commessa e la sanzione irrogata sono garantiti dal rispetto dei seguenti criteri:

- gravità della violazione commessa;
- mansione, ruolo, responsabilità e autonomia del dipendente;
- prevedibilità dell'evento;
- intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia;
- comportamento complessivo dell'autore della violazione, con riguardo alla sussistenza o meno di precedenti disciplinari nei termini previsti dal CCNL applicabile;
- al concorso, nella violazione commessa, di più lavoratori in accordo tra loro;
- altre particolari circostanze che caratterizzano la violazione.

È inteso che saranno seguite tutte le disposizioni e le garanzie previste dal CCNL in materia di procedimento disciplinare.

In particolare si osserverà:

- l'obbligo della previa contestazione dell'addebito al dipendente con indicazione dei fatti costitutivi dell'infrazione e del termine, dal ricevimento della contestazione entro cui il dipendente potrà presentare le proprie giustificazioni, e dell'audizione di quest'ultimo in ordine alla sua difesa;
- l'obbligo di non adottare il provvedimento disciplinare, se più grave del rimprovero verbale, prima che sia trascorso il termine minimo previsto dall'art. 7 dello Statuto dei Lavoratori dalla contestazione per iscritto dell'addebito, nel corso del quale il lavoratore può presentare le proprie giustificazioni;
- l'obbligo di comunicazione dell'adozione del provvedimento disciplinare per iscritto, entro e non oltre i termini massimi previsti dai rispettivi CCNL, dalla scadenza del termine assegnato al dipendente per la presentazione delle sue giustificazioni. In caso contrario, il procedimento disciplinare è definito con l'archiviazione.

L'esistenza di un sistema sanzionatorio connesso al mancato rispetto delle disposizioni contenute nel Modello e nella documentazione che di esso forma parte, deve essere, necessariamente, portato a conoscenza del personale dipendente attraverso i mezzi ritenuti più idonei dalla Società.

5.2 Sanzioni nei confronti dei dirigenti

In caso di violazione, da parte di Dirigenti, delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività a rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, si

provvederà ad applicare nei confronti dei responsabili le idonee misure in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti applicabile. Laddove la violazione sia tale da far venir meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

5.3 Misure nei confronti degli Amministratori e dei Sindaci

L'O.d.V. informa il Presidente del Consiglio di Amministrazione e il Presidente del Collegio Sindacale delle segnalazioni aventi ad oggetto violazioni del Modello o del Codice Etico da parte degli Amministratori e dei Sindaci che non siano state ritenute, manifestamente, infondate affinché provvedano a investire della questione gli organi da essi presieduti. Si applicano gli articoli 2392 e 2407 del codice civile.

5.4 Misure nei confronti dei membri dell'O.d.V.

In caso di violazioni del presente Modello da parte di uno o più componenti dell'O.d.V., gli altri componenti dell' O.d.V. ovvero uno qualsiasi tra i sindaci o tra gli amministratori informano, immediatamente, il Collegio Sindacale ed il Consiglio di Amministrazione della Società. Tali organi, previa contestazione della violazione e preso atto delle argomentazioni difensive eventualmente addotte, assumono gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico.

5.5 Misure nei confronti di Fornitori, Collaboratori, Partner e Consulenti

La violazione da parte di Collaboratori esterni alla Società, di Soci in società ed enti partecipati dalla Società, di Fornitori di beni e servizi e Partner, delle norme previste dal Decreto 231 e/o dal Codice Etico, può essere causa di risoluzione del contratto. La violazione va denunciata senza indugio al Consiglio di Amministrazione ovvero all'Amministratore Delegato da parte di chi la rileva. Se il Consiglio di Amministrazione o l'Amministratore Delegato ritiene che la denuncia sia fondata, può ordinare l'immediata risoluzione del contratto e ne dà notizia all' O.d.V. Egli dà, ugualmente, notizia all'O.d.V. dei casi in cui egli non proceda a risolvere il contratto perché ritiene non fondata la denuncia o perché la risoluzione sarebbe di grave danno per la Società.

La risoluzione del contratto comporta l'accertamento dei danni che la Società abbia, eventualmente, subito e la conseguente azione di risarcimento.