Modello Organizzativo ai sensi del

Decreto Legislativo 8 giugno 2001, n. 231

Rev.	Approvazione	Natura delle modifiche
00	Consiglio di Amministrazione 22/09/21	Adozione
01	Consiglio di Amministrazione 13/09/23	Aggiornamento

CY4GATE S.p.A. – Part of ELT Group
Sede Legale Via Coponia 8, 00131 Roma
Capitale Sociale Euro 1.441.499,94
Registro Imprese di Roma, Codice Fiscale, Partita Iva 13129151000
REA RM-1426295
www.cy4gate.com – www.elettronicagroup.com

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.

Il Decreto tuttavia, se da un lato disegna un rigido schema repressivo, dall’altro predispone un’evidente attenuazione di tale rigore per l’ente che si sia dotato di idonei sistemi di prevenzione dei reati dai quali discende la responsabilità delle persone

giuridiche. L'obiettivo è quello di spingere le persone giuridiche a dotarsi di un'organizzazione interna in grado di prevenire le condotte delittuose. L'ente, infatti, non risponde se prova di avere adottato le misure, indicate dallo stesso legislatore, che si presumono idonee alla funzione di prevenzione.
Le condizioni essenziali perché sia configurabile la responsabilità dell'ente sono tre:

- sia stato commesso un reato a cui la legge collega la responsabilità dell'ente;
- il reato sia stato commesso nell'interesse o a vantaggio dell'ente stesso;
- l'autore del reato, ovvero colui che provoca la «responsabilità amministrativa» della Società nella quale o per la quale egli opera sia:
    - soggetto apicale, ossia colui il quale riveste funzioni di rappresentanza, di amministrazione o di direzione della Società, nonché colui che esercita, anche di fatto, la gestione e il controllo delle stesse;
    - soggetto sottoposto alla direzione o alla vigilanza di soggetti apicali.

La responsabilità dell'ente, pertanto, discende dalla commissione, da parte di soggetti ad esso appartenenti, di reati tassativamente indicati dal decreto 231 ovvero, in base a quanto disposto dall'art. 2, qualora la sua responsabilità sia prevista da altra legge che sia entrata in vigore prima della commissione del fatto.

Inoltre, il D.Lgs. 231/2001 differenzia la disciplina del criterio di imputazione operante sul piano subiettivo a seconda che il reato sia commesso da un soggetto in posizione apicale o da un semplice sottoposto.

Il decreto inoltre sancisce il principio di autonomia della responsabilità dell'ente da quella della persona fisica, precisando che la responsabilità dell'ente sussiste anche quando:

- l'autore del reato non è stato identificato o non è imputabile;
- il reato si estingue per una causa diversa dall'amnistia.

La suddetta responsabilità si configura anche in relazione a reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'ente abbia nel territorio dello Stato italiano la sede principale.

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 Ministero 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"*.

1.2 l'adozione dei modelli di organizzazione, gestione e controllo quali esimenti della responsabilità amministrativa dell'ente

Alla luce dell'art. 5, comma II, D.Lgs. 231/2001 l'ente non risponde se i soggetti attivi hanno agito nell'interesse esclusivo proprio o di terzi.

Inoltre, l'art. 6 specifica che la Società non risponde se prova che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dotato di autonomi poteri di iniziativa e di controllo;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo a questo preposto.

Il D.Lgs. 231/01 definisce, inoltre, i requisiti dell'efficace attuazione dei modelli organizzativi che devono:

- individuare 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 di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
- verificare periodicamente e eventualmente modificare il modello quando siano scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione e nell'attività;
- prevedere un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- prevedere uno o più canali per la segnalazione delle condotte illecite, di cui uno idoneo a garantire con modalità informatiche la riservatezza dell'identità del segnalante;
- prevedere il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

La mera adozione di un modello non è sufficiente ad escludere la responsabilità dell'ente, essendo necessario che il modello sia effettivamente ed efficacemente attuato. In particolare, l'efficace attuazione del modello richiede, in aggiunta alla concreta applicazione del sistema disciplinare, anche una verifica periodica sul modello stesso e l'aggiornamento/modifica dello stesso nel caso siano scoperte significative violazioni delle sue prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività dell'ente.

1.3 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.

Le fattispecie di reato oggi suscettibili di configurare la responsabilità amministrativa della Società, se commessi nel suo interesse o a suo vantaggio dai soggetti sopra menzionati, sono espressamente richiamate dagli artt. 24 a 26 del D.Lgs. 231/01, nonché dalla L. 146/2006 e dalla L. 9/2013.

Un elenco completo dei reati suscettibili di configurare la responsabilità amministrativa della Società è riportato nell' **allegato 1** del presente Modello con indicazione delle fattispecie applicabili e relativa descrizione della normativa di riferimento.

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.

Le sanzioni pecuniarie sono calcolate 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, (applicabili anche in via cautelare) di durata non inferiore a tre mesi e non superiore a sette anni (con la precisazione che, ai sensi dell'art. 14, comma 1, d.lgs. 231/01, "*Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente*") che, a loro volta, possono consistere in:

- interdizione dell'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.

Si rappresenta, altresì, che ai sensi del D.L n. 2/2023, qualora sussistano i presupposti per l'applicazione di una sanzione interdittiva che possa determinare l'interruzione dell'attività di un impianto di interesse strategico nazionale, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente tramite un commissario. Non possono essere applicate sanzioni interdittive qualora l'ente abbia adottato un modello organizzativo coerente con quelli delineati nei provvedimenti relativi alla procedura di riconoscimento dell'interesse strategico nazionale diretti a realizzare il necessario bilanciamento tra esigenze di continuità dell'attività produttiva e di salvaguardia degli altri beni giuridici protetti dall'ordinamento.

SEZIONE SECONDA

IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI CY4GATE

2.1. La Società

CY4gate opera nel settore della progettazione, sviluppo e produzione di tecnologie nell'ambito dei settori della cyber security e cyber intelligence a favore di enti Istituzionali e aziende Corporate.

Con riferimento alla cyber intelligence, 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 cyber security, la società realizza prodotti finalizzati alla protezione dei sistemi informatici dei propri clienti, ma anche all'analisi ed alla catalogazione delle minacce, proponendo misure di contrasto.

L'offerta commerciale della società si declina a sua volta in tre diverse linee di business: decision intelligence, cyber security e forensic intelligence; quest'ultima è esclusivamente rivolta a clienti istituzionali.

2.2. Contesto organizzativo interno

Il sistema organizzativo definisce l'articolazione organizzativa della struttura della Società, ossia unità, ruoli e posizioni organizzative, individua i responsabili e descrive le relative aree di responsabilità assegnate nel rispetto del principio di segregazione delle funzioni così come degli altri principi di compliance e governance.

Le risorse umane della Società sono ripartite nelle seguenti principali aree, all'interno delle quali si identificano le funzioni dei dirigenti, che impartiscono le direttive.

Nel dettaglio, a diretto riporto dell'Amministratore Delegato (di seguito anche AD), vengono collocate le seguenti strutture e funzioni:

- **Strutture Organizzative Tecniche:** Cyber & Decision Intelligence Engineering e Forensic Intelligence Engineering;
- **Strutture Operations:** Cyber Security Operations e Portfolio & Planning Management;
- **Strutture Commerciali**: Marketing & Sales Italy; Defense & Security Sales Italy; Defense & Security Sales Italy, International Sales;
- **Strutture di Staff:** Group Accounting, Finance, Controlling and Procurement e Group HR, Legal & Shared Services.

Infine, per la peculiarità del ruolo, responsabilità e deleghe affidate, riportano funzionalmente all'AD: il Chief Information Security Officer e il Chief Security Officer.

In qualità di *Advisor* dell'Amministratore Delegato, altresì, operano:

- il Data Protection Officer (di seguito anche DPO);
- il Responsabile del Servizio Prevenzione e Protezione (di seguito anche RSPP).

2.3. Poteri e deleghe interni

A norma di Statuto, spettano tutti i poteri per l'ordinaria e straordinaria amministrazione della CY4gate al Consiglio di Amministrazione (di seguito CdA), il quale ha delegato alcune delle proprie attribuzioni all'Amministratore Delegato (di seguito AD), al fine di assicurare unitarietà alla gestione corrente, in attuazione a quanto deliberato dal Consiglio stesso. Inoltre, il CdA ha definito l'ambito dei poteri deliberativi e di spesa conferiti ai responsabili delle strutture organizzative, in coerenza con le responsabilità organizzative e gestionali attribuite, predeterminandone i limiti e fissando altresì modalità e limiti per l'esercizio delle subdeleghe.

La facoltà di subdelega è esercitata attraverso un processo trasparente, sempre monitorato, graduato in funzione del ruolo e della posizione ricoperta dal "subdelegato", comunque prevedendo l'obbligo di informativa alla funzione delegante.

Sono inoltre formalizzate le modalità di firma sociale per atti, contratti, documenti e corrispondenza, sia esterna che interna e le relative facoltà sono attribuite ai dirigenti o dipendenti in forma abbinata o singola.

Tutte le strutture operano sulla base di specifiche procedure, che definiscono i rispettivi ambiti di competenza e di responsabilità; tali procedure sono emanate e portate a conoscenza nell'ambito della CY4gate.

Anche le procedure operative, che regolano le modalità di svolgimento dei diversi processi aziendali, sono diramate all'interno della CY4gate attraverso specifiche procedure. Pertanto, i principali processi decisionali ed attuativi riguardanti l'operatività di CY4gate sono codificati, monitorabili e conoscibili da tutta la struttura.

2.4. Il Modello 231 adottato da CY4gate

È politica di CY4gate diffondere a tutti i livelli una cultura generale orientata al rispetto delle norme e al controllo interno, come definito nel Codice Etico (All.3). L'adozione e il continuo aggiornamento del presente Modello di Organizzazione e di Gestione ai sensi del D.Lgs. 231/01 risponde all'esigenza di indirizzare l'operato della società in tal senso, per quanto più specificatamente attinente i "processi sensibili" connessi con i reati – presupposto ex D.lgs. 231/01.

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.

Il Modello si ispira ai principi e alle best practices più avanzate nel campo della lotta alla criminalità d'impresa e si uniforma ai principi di controllo elaborati dalle Linee Guida di Confindustria.

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;
- adotta 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;
- prevede un sistema di controllo interno e di gestione dei rischi e individua i processi di controllo e gestione delle risorse finanziarie, adeguati a prevenirne gli utilizzi inadeguati con riferimento particolare ai reati oggetto del D. Lgs. 231/01;
- attribuisce all' Organismo di Vigilanza (di seguito anche OdV) il compito di vigilare sul funzionamento del Modello 231, sul controllo dell'osservanza e sulle opportunità di aggiornamento.

Nel presente documento, CY4gate ha proceduto all'aggiornamento del Modello al fine di renderlo rispondente alla nuova situazione aziendale di CY4gate, tra cui l'acquisizione di nuove società nonché il passaggio sul mercato regolamentato Euronext Milan- segmento STAR- organizzato e gestito da Borsa Italiana S.p.A., alle novità legislative, all'evoluzione della giurisprudenza e delle *best practices* nazionali ed internazionali.
Il presente Modello entra in vigore a decorrere dalla data della sua approvazione da parte del Consiglio di Amministrazione di CY4gate.

Il Modello è rivolto a tutti i Destinatari e le eventuali violazioni dello stesso potranno dar luogo all'applicazione di specifiche misure, così come previsto alla sezione quinta della presente Parte Generale.

2.5. Struttura del Modello

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

- una sintetica descrizione del quadro normativo, integrata dalle fattispecie di reato, riportate in apposito allegato;
- una breve presentazione della Società, la natura, metodologia e struttura del modello 231 adottato da CY4gate, i suoi elementi fondamentali, gli allegati, compreso il Codice Etico, i destinatari, nonché il sistema di controllo interno di gestione e di gestione dei rischi e le regole che disciplinano le modalità di diffusione e aggiornamento del Modello;
- le regole riguardanti la costituzione dell'OdV;
- le sanzioni applicabili in caso di violazioni delle regole e delle prescrizioni contenute nel Modello;
- il sistema di segnalazione delle violazioni (*whistleblowing*).

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.

2.6. 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.).

2.7. Metodologia

2.7.1 Identificazione analitica delle attività sensibili e delle aree critiche.

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.

La mappatura delle aree esposte a rischio di realizzazione di reati-presupposto è effettuata mediante un processo di autovalutazione (Risk Assessment) seguendo le seguenti fasi:

- analisi della realtà aziendale, delle caratteristiche della società e delle tipologie di attività effettivamente esercitate;
- analisi delle attività sensibili, volte ad individuare gli ambiti e i processi a rischio;
- analisi dell'esistente sistema di controllo interno;
- analisi della normazione interna (procedure interne);
- analisi dei sistemi di rendicontazione (es. report, verbali, segnalazioni);
- analisi dell'assetto organizzativo (organigramma, procure, documenti esistenti);
- interviste ai soggetti muniti di poteri decisionali e di spesa/ responsabili di funzione.

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.

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).

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.

Come meglio descritto nella Sezione Quarta del presente Modello, 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.

2.7.2. Implementazione del Modello e la valutazione del rischio

La metodologia d'implementazione 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 CY4gate, 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 e in genere alle attività di business della Società, distinguendo per i reati inerenti i comportamenti finali dalle condotte;
- 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'effettuazione della gap analysis. Rendicontazione delle attività svolte in sede di mappatura dei rischi e degli esiti delle interviste, nonché rendicontazione delle attività di audit effettuate. Vengono indicate le aree di rischio ritenute rilevanti nelle singole parti speciali. Sono individuati gli interventi migliorativi o correttivi (creazione o implementazione delle procedure interne; predisposizione di nuove deleghe e/o procure o revisione dell'assetto preesistente). Infine, viene predisposto un documento di sintesi in un file excel (mappatura dei rischi).

2.8. Il sistema di controllo interno e di gestione dei rischi di CY4gate

Il sistema di controllo interno e di gestione dei rischi (di seguito anche SCIGR) è costituito dall'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società.

Un efficace SCIGR contribuisce a una conduzione dell'impresa coerente con gli obiettivi aziendali definiti dal Consiglio di Amministrazione, favorendo l'assunzione di decisioni consapevoli. Esso concorre ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità delle informazioni fornite agli organi sociali ed al mercato, il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne.

Gli attori del SCIGR agiscono secondo un modello a tre livelli di controllo:

- il primo livello di controllo: identifica, valuta, gestisce e monitora i rischi di competenza in relazione ai quali individua e attua specifiche azioni di trattamento. La responsabilità di definire ed effettuare tali controlli è del management, opera ad ogni livello della struttura organizzativa e si esplica nel quadro della gestione corrente;
- il secondo livello di controllo: monitora i principali rischi per assicurare l'efficacia e l'efficienza del loro trattamento, monitora l'adeguatezza e l'operatività dei controlli posti a presidio dei principali rischi e, inoltre, fornisce supporto al primo livello nella

definizione e implementazione di adeguati sistemi di gestione dei principali rischi e dei relativi controlli;

- il terzo livello di controllo: fornisce “assurance” indipendente e obiettiva sull’adeguatezza e sull’effettiva operatività del primo e secondo livello di controllo e, in generale, sul SCIGR nel suo complesso. È svolto da unità indipendenti, diverse da quelle operative, quali l’Internal audit.

CY4gate adotta il modello di amministrazione e controllo tradizionale, anche in linea con il Codice di Corporate Governance 2020 delle Società Quotate cui CY4gate ha aderito, 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 e assistito da comitati endo-consiliari; (ii) di gestione, demandata all’Amministratore Delegato (di seguito anche AD); (iii) di controllo, svolta dal Collegio Sindacale.

In particolare:

(i) il Consiglio di Amministrazione (di seguito anche CdA) a) definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi in coerenza con le strategie della società e valuta, con cadenza almeno annuale, l’adeguatezza del medesimo sistema rispetto alle caratteristiche dell’impresa e al profilo di rischio assunto, nonché la sua efficacia; b) nomina e revoca il responsabile della funzione di internal audit, definendone la remunerazione coerentemente con le politiche aziendali, e assicurandosi che lo stesso sia dotato di risorse adeguate all’espletamento dei propri compiti. Qualora decida di affidare la funzione di internal audit, nel suo complesso o per segmenti di operatività, a un soggetto esterno alla società, assicura che esso sia dotato di adeguati requisiti di professionalità, indipendenza e organizzazione e fornisce adeguata motivazione di tale scelta nella relazione sul governo societario; c) approva, con cadenza almeno annuale, il piano di lavoro predisposto dal responsabile della funzione di internal audit, sentito l’organo di controllo e l’AD; d) valuta l’opportunità di adottare misure per garantire l’efficacia e l’imparzialità di giudizio delle altre funzioni aziendali, verificando che siano dotate di adeguate professionalità e risorse; e) attribuisce all’organismo appositamente costituito le funzioni di vigilanza ex art. 6, comma 1, lett. b) del Decreto Legislativo n. 231/2001. Nel caso l’organismo non coincida con l’organo di controllo,

l'organo di amministrazione valuta l'opportunità di nominare all'interno dell'organismo almeno un amministratore non esecutivo e/o un membro dell'organo di controllo e/o il titolare di funzioni legali o di controllo della società, al fine di assicurare il coordinamento tra i diversi soggetti coinvolti nel sistema di controllo interno e di gestione dei rischi; f) valuta, sentito l'organo di controllo, i risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione aggiuntiva indirizzata all'organo di controllo; g) descrive, nella relazione sul governo societario, le principali caratteristiche del sistema di controllo interno e di gestione dei rischi e le modalità di coordinamento tra i soggetti in esso coinvolti, indicando i modelli e le best practice nazionali e internazionali di riferimento, esprime la propria valutazione complessiva sull'adeguatezza del sistema stesso e dà conto delle scelte effettuate in merito alla composizione dell'organismo di vigilanza di cui alla precedente lettera e). Esamina ed approva le operazioni ordinarie e straordinarie, nonché i piani strategici della società. A seguito del passaggio sul mercato regolamentato Euronext Milan- segmento STAR- organizzato e gestito da Borsa Italiana S.p.A., il Consiglio di Amministrazione potrà essere formato da 7 a 9 membri di cui almeno un terzo indipendenti ed almeno il 40% in rappresentanza del genere meno rappresentato.

Si rappresenta, altresì, che il CdA di CY4gate ha costituito 4 comitati endo-consiliari con funzione consultativa e propositiva, che garantiscono ulteriori presidi di controllo:

- ***Il Comitato controllo rischi e sostenibilità (di seguito Comitato CRS),*** composto da almeno tre amministratori, non esecutivi, in maggioranza indipendenti secondo i requisiti di indipendenza previsti dal Codice di Corporate Governance, di cui il Presidente è scelto fra gli amministratori indipendenti.

  Nello specifico il Comitato CRS ha il compito di:

  (i) assistere il CdA con funzioni istruttorie, propositive e consultive, nelle valutazioni e nelle sue decisioni relative al sistema di controllo interno e di gestione dei rischi, nonché quelle riguardanti le questioni di sostenibilità.

  (ii) Il Comitato CRS, nel coadiuvare l'organo di amministrazione: a) valuta il revisore legale e l'organo di controllo, il corretto utilizzo dei princìpi contabili e, nel caso di gruppi, la loro omogeneità ai fini della redazione del bilancio consolidato; b) valuta l'idoneità dell'informazione periodica, finanziaria e non finanziaria, a rappresentare correttamente il modello di business, le

strategie della società, l'impatto della sua attività e le performance conseguite, esamina il contenuto dell'informazione periodica a carattere non finanziario rilevante ai fini del SCIGR; d) esprime pareri su specifici aspetti inerenti alla identificazione dei principali rischi aziendali e supporta le valutazioni e le decisioni dell'organo di amministrazione relative alla gestione di rischi derivanti da fatti pregiudizievoli di cui quest'ultimo sia venuto a conoscenza; e) esamina le relazioni periodiche e quelle di particolare rilevanza predisposte dalla funzione di Internal audit; f) monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della funzione di internal audit; g) può affidare alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al presidente dell'organo di controllo; h) riferisce all'organo di amministrazione, almeno in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta e sull'adeguatezza del sistema di controllo interno e di gestione dei rischi.

Il Comitato, inoltre, esamina e valuta:

(i) le comunicazioni e le informazioni ricevute dal Collegio Sindacale e dai suoi componenti in merito al SCIGR;

(ii) le relazioni annuali emesse dall'Organismo di Vigilanza, nonché le informative tempestive rese dallo stesso, previa informativa alla Presidente del Consiglio di Amministrazione e all'Amministratore Delegato, in merito a eventuali fatti di particolare materialità o significatività accertati nell'esercizio dei compiti ad esso assegnati.

- ***il Comitato Nomine e remunerazioni*** che assiste il CdA con compiti, di natura istruttoria, propositiva e consultiva in materia di nomine e remunerazioni. Il Comitato è composto da almeno tre amministratori, non esecutivi, in maggioranza indipendenti secondo i requisiti di indipendenza previsti dal Codice di Corporate Governance. Il Presidente è scelto fra gli amministratori indipendenti;
- ***il Comitato Parti correlate*** che ha il compito di esprimere il proprio parere sulle operazioni con parti correlate, in conformità alle specifiche procedure approvate dal CdA. Il Comitato è composto da amministratori non esecutivi, in maggioranza

indipendenti secondo i requisiti di indipendenza previsti dal Codice di Corporate Governance;

- ***il Comitato Strategico*** che assiste il CdA e gli organi delegati della Società con funzioni istruttorie, propositive e consultive, nelle valutazioni e nelle sue decisioni secondo le specifiche competenze allo stesso attribuite, fermo restando che la valutazione circa l'approvazione delle possibili operazioni prospettate dal Comitato spetta esclusivamente al CdA. Il Comitato è composto da almeno tre membri. L'AD è di diritto membro del Comitato mentre i restanti membri del Comitato vengono nominati dal CdA e scelti tra i componenti del medesimo.

(ii) l'Amministratore delegato incaricato dell'istituzione e del mantenimento del sistema di controllo interno e di gestione dei rischi a) cura l'identificazione dei principali rischi aziendali, tenendo conto delle caratteristiche delle attività svolte dalla società e dalle sue controllate, e li sottopone periodicamente all'esame dell'organo di amministrazione; b) dà esecuzione alle linee di indirizzo definite dall'organo di amministrazione, curando la progettazione, realizzazione e gestione del sistema di controllo interno e di gestione dei rischi e verificandone costantemente l'adeguatezza e l'efficacia, nonché curandone l'adattamento alla dinamica delle condizioni operative e del panorama legislativo e regolamentare; c) può affidare alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative e sul rispetto di regole e procedure interne nell'esecuzione di operazioni aziendali, dandone contestuale comunicazione al presidente dell'organo di amministrazione, al presidente del comitato controllo e rischi e al presidente dell'organo di controllo; d) riferisce tempestivamente al comitato controllo e rischi in merito a problematiche e criticità emerse nello svolgimento della propria attività o di cui abbia avuto comunque notizia, affinché il comitato possa prendere le opportune iniziative.

(iii) 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'attività di vigilanza sul generale processi di gestione dei rischi aziendali è svolta attraverso incontri con responsabili delle principali aree di business e delle principali aree funzionali, la partecipazione alle riunioni del CdA e degli altri Comitati consiliari e lo scambio di informazione con la Società di Revisione. Il Collegio, inoltre, collabora periodicamente con l'OdV.

2.8.1. Principali soggetti coinvolti nel SCIGR

Di seguito vengono riportate una descrizione dei compiti e delle responsabilità dei principali soggetti coinvolti in ambito SCIGR e 231:

La Funzione Internal audit

A seguito del passaggio dal segmento Euronext Growth Milan allo STAR, CY4Gate ha stabilito di dotarsi di una propria Funzione Internal audit (di seguito anche IA) che dipende gerarchicamente dall'organo di amministrazione. In linea con quanto ammesso dal Codice di Corporate Governance, CY4Gate ha deciso di affidare tale funzione in outsourcing ad un soggetto esterno dotato dei requisiti di professionalità, indipendenza e organizzazione. l'IA valuta l'efficacia e l'adeguatezza del SCIGR, attraverso un piano di audit, approvato dal CdA e dal Comitato CRS, basato su un processo strutturato di analisi e prioritizzazione dei principali rischi. Predispone e condivide relazioni periodiche contenenti adeguate informazioni sulla propria attività, sulle modalità con cui viene condotta la gestione dei rischi nonché sul rispetto dei piani definiti per il loro contenimento. Verifica, nell'ambito del piano di audit, l'affidabilità dei sistemi informativi.

La Funzione Internal Audit facilita il coordinamento con le funzioni di controllo di II livello e mantiene canali informativi diretti nei confronti dell'Amministratore Delegato, del Dirigente Preposto, del Comitato Controllo e Rischi e Sostenibilità, del Collegio Sindacale e dell'Organismo di Vigilanza, ai quali ha accesso diretto e con i quali comunica senza restrizioni o intermediazioni.

L'IA ha, pertanto, il compito di: (i) verificare l'operatività e l'adeguatezza del SCIGR, sia in via continuativa sia in relazione a specifiche necessità e di fornire valutazioni e raccomandazioni al fine di promuoverne l'efficienza e l'efficacia; (ii) fornire supporto specialistico al management in materia di SCIGR al fine di favorire l'efficacia, l'efficienza e l'integrazione dei controlli nei processi aziendali e promuovere il costante miglioramento della governance e del risk management.

L'Organo di Coordinamento e Consultazione per la Prevenzione della Corruzione

Raccomanda al CdA eventuali aggiornamenti o modifiche del Codice Anticorruzione (**All.3**) con particolare riguardo all'evoluzione delle *best practice* emergenti e della normativa di riferimento ovvero in caso di riscontrate criticità. Le successive modifiche e

integrazioni del Codice Anticorruzione competono, pertanto, al CdA ad eccezione di quelle formali che verranno apportate dall'Organo di Coordinamento e Consultazione per la Prevenzione della Corruzione avvalendosi delle unità organizzative Human Resources, Legal, Anticorruzione e Finance.

La funzione Antiriciclaggio

In linea con la Policy Antiriciclaggio di CY4gate (**All.4**), che verifica nel continuo che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione delle e norme regolamentari e di autoregolamentazione in materia di riciclaggio, di finanziamento al terrorismo, di violazione degli embarghi, della normativa armamenti- e anticorruzione. Per il perseguimento delle finalità di cui al D. Lgs. 231/2001, la funzione Antiriciclaggio limitatamente alla gestione dei rischi in materia di antiriciclaggio, di finanziamento del terrorismo, di violazione degli embarghi, della normativa armamenti e anticorruzione:

- partecipa alla definizione della struttura del Modello e all'aggiornamento dello stesso;
- promuove le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio di riciclaggio e di finanziamento del terrorismo;
- riceve e inoltra i reporting periodici e i flussi informativi previsti dalle "Linee Guida per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi";
- cura, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di adeguate attività formative, finalizzate a conseguire un aggiornamento su base continuativa dei dipendenti e dei collaboratori.

La funzione finance

Il Chief Financial Officer (CFO) coordina e definisce le linee guida di gestione in ambito amministrativo-finanziario per tutte le società del gruppo in concerto con le altre funzioni dirigenziali. Il suo ruolo consiste, a:

- presidiare il processo di gestione amministrativa/ finanziaria e i controlli sottostanti in modo da garantire il corretto funzionamento delle Società in modo

da coordinare e dare supporto alle società del gruppo e alle direzioni che gestiscono il core business;
- garantire la compliance alla normativa fiscale e civilistica di riferimento coordinando risorse interne ed esterne.

Le funzioni della posizione sono di seguito riportate:

- Amministrare le legal entities (LE) del Gruppo negli aspetti civilistici, fiscali, economici, finanziari e di reporting.
- Supervisionare e controllare il funzionamento delle procedure amministrative, gestionali e fiscali per una corretta informazione e valutazione della gestione.
- Supervisionare l'adempimento degli obblighi fiscali e la tenuta di tutti i libri obbligatori e la loro regolarità fiscale anche mediante l'ausilio di professionisti esterni abilitati e da lui scelti.
- Supervisionare le attività necessarie per l'espletamento della revisione legale dei bilanci di esercizio delle LE del Gruppo e del bilancio consolidato del Gruppo.
- Supervisionare le attività necessarie per dare pronta risposta alle richieste del Collegio Sindacale e dell'Organismo di Vigilanza.
- Curare gli aspetti legali, patrimoniali e societari, che interessano la società potendo contare, in caso di necessità, su consulenze e contributi di personale qualificato esterno.
- Effettuare il controllo continuo del rispetto delle procedure aziendali del settore amministrazione con tempestiva segnalazione delle eventuali anomalie alle funzioni preposte.
- Garantire la corretta interfaccia con Borsa Italiana e i relativi organi di vigilanza.
- Assistere revisori/consulenti coinvolti in specifiche operazioni societarie (es. fusioni, e acquisizioni, due diligence, nuove incorporazioni, operazioni su azioni/attività ecc.).
- Definire le politiche e le strategie aziendali a lungo termine.
- Definire gli indirizzi e gli obiettivi delle strutture aziendali sottostanti.
- Attuare un controllo generale sulla gestione dell'azienda.
- Affidare incarichi speciali ai propri membri o all'esterno.

Si rappresenta, inoltre, che la funzione finance ha curato la redazione del prospetto

informativo in forma semplificata ai sensi dell'art. 14, lett. d), del regolamento (UE) n. 1129/2017, del Regolamento Delegato (UE) 979/2019 e del Regolamento Delegato (EU) 980/2019, depositato presso la Consob e disponibile sul sito internet della società, che fornisce le informazioni chiave di cui gli investitori necessitano per comprendere la natura e i rischi di CY4gate, del Gruppo e delle azioni ordinarie che sono ammesse alla negoziazione sul mercato regolamentato Euronext Milan- segmento STAR- organizzato e gestito da Borsa Italiana S.p.A..

Il Dirigente Preposto

In ottemperanza alle previsioni di cui all'art. 154-bis del TUF (Legge n. 262 del 28 dicembre 2005 "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari"), il Consiglio di Amministrazione ha nominato il C.F.O. della Società dirigente preposto alla redazione dei documenti contabili societari avente le funzioni previste dal citato articolo del TUF e a cui conferire adeguati poteri e mezzi per l'esercizio dei compiti attribuiti dalle disposizioni di legge e regolamentari di volta in volta vigenti, anche in considerazione dei requisiti disposti dalla normativa applicabile e dallo statuto sociale entrati in vigore con la quotazione su Euronext Milan – Segmento STAR.

Il Dirigente Preposto redige una relazione sulle attività svolte nel periodo di riferimento che viene trasmessa al CdA al momento dell'approvazione del progetto di bilancio, e rilascia, a firma congiunta con l'AD, le Attestazioni sul bilancio di esercizio e sul bilancio consolidato ai sensi dell'art. 154 bis, secondo gli schemi Consob. In particolare, attesta:

- l'adeguatezza delle procedure amministrative e contabili per la formazione del bilancio di esercizio e del bilancio consolidato;
- l'effettiva applicazione delle procedure nel corso del periodo cui si riferiscono i documenti di bilancio;
- la corrispondenza dei bilanci alle risultanze dei libri e delle scritture contabili;
- l'idoneità dei bilanci a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria della società e delle partecipate incluse nel consolidamento;
- che la relazione sulla gestione comprenda un'analisi attendibile dell'andamento e del risultato della gestione, nonché della situazione dell'emittente e dell'insieme

delle imprese incluse nel consolidamento, unitamente alla descrizione dei principali rischi e incertezze cui sono esposte.

In aggiunta, si evidenzia che la funzione finance e la funzione del Dirigente preposto si integrano con gli altri modelli di controllo e di gestione del rischio, implementati in CY4gate e nel gruppo, nell'ottica di un SCIGR sempre più integrato, come a titolo esemplificativo, con il Modello di Controllo di gestione di cui al punto 2.8.2.

La funzione Legal

Per il perseguimento delle finalità di cui al D. Lgs. 231/2001, assicura assistenza e consulenza legale alle strutture aziendali, seguendo l'evolversi della normativa specifica e degli orientamenti giurisprudenziali in materia. Spetta altresì alla funzione Legale l'interpretazione della normativa, la risoluzione di questioni di diritto e l'identificazione delle condotte che possono configurare ipotesi di reato. La funzione Legale collabora con le funzioni Internal audit, Risorse Umane, Antiriciclaggio, con il Datore di lavoro ai sensi del D. Lgs. 81/2008, all'adeguamento del Modello, segnalando anche eventuali estensioni dell'ambito di responsabilità amministrativa degli enti.

Il DPO

In ottemperanza a quanto previsto dal Regolamento UE 2016/679 (General Data Protection Regulation – "GDPR"), CY4gate si è dotata di un proprio sistema gestionale per la protezione dei dati personali. Il sistema di gestione privacy definisce il set di regole interne, le metodologie, i ruoli e le responsabilità attribuiti a tutte le strutture coinvolte nel trattamento di dati personali. Come da Regolamento UE 2016/679, il Data Protection Officer è tenuto a sorvegliare l'osservanza del Regolamento e delle altre disposizioni di legge relative alla protezione dei dati, configurandosi a tutti gli effetti come un elemento del sistema di Controllo interno e Gestione dei Rischi.

Il sistema di gestione privacy prevede altre norme interne che indirizzano le attività da porre in essere per garantire la compliance alle previsioni del Regolamento. Sono regolamentati gli aspetti relativi alla data protection by design e by default, al processo di data protection impact assessment, alla gestione dei data breach, all'attuazione dei tempi di cancellazione dei dati, alla gestione dei diritti degli interessati.

La società di revisione legale dei conti

CY4gate è, inoltre, sottoposta all'attività di revisione legale dei conti da parte della società di revisione individuata dall'assemblea pro-tempore sia per quanto riguarda le informazioni finanziarie sia per quanto riguarda le informazioni non finanziarie.

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.

2.8.2. I sistemi di gestione e controllo dei rischi specifici

Sul piano più propriamente operativo non possono essere sottaciuti, in quanto fondamentali strumenti di prevenzione di cui il Modello 231 si avvale per le proprie finalità cautelari, i vari Sistemi di Gestione e controllo di rischi specifici adottati in azienda:

- ***Sistema di Controllo di Gestione (di seguito anche SCG)***: si intende l'insieme strutturato ed integrato di informazioni e processi utilizzato dal management a supporto delle attività di pianificazione e controllo, coerentemente al Business Model del Gruppo CY4gate (di seguito il Gruppo). Il SCG del Gruppo è finalizzato a supportare il Management nella pianificazione e nel monitoraggio degli obiettivi economico-finanziario-patrimoniali attraverso la funzione Finance.

  Il CFO e la funzione Pianificazione e Controllo di Gestione della capogruppo, attraverso le differenti attività svolte forniscono il supporto e gli strumenti necessari a:

  ❖ definire gli obiettivi e supportare le decisioni relative a:
    - identificazione della strategia e degli obiettivi di business;
    - individuazione delle linee guida e del piano di azione per raggiungere gli obiettivi;
    - valutazione dei Fattori Critici di Successo (FCS) e dei Fattori Critici di Rischio (FCR);

- ❖ monitorare i seguenti aspetti:
  - raggiungimento degli obiettivi strategici formalizzati nel Business Plan;
  - FCS che consentono il raggiungimento di tali obiettivi;
  - FCR che influenzano il raggiungimento dei medesimi;
  - efficacia ed efficienza di processi e funzioni;
- ❖ implementare le azioni correttive a seguito di eventuali scostamenti, positivi o negativi, tra i consuntivi e gli obiettivi.

Il SCG si articola su differenti livelli e dimensioni:

- ❖ oggetti di controllo, che rappresentano il "*cosa controllare*" e sono costituiti da:
  - indicatori e metriche;
  - dimensioni di analisi (descritte nel seguito);
- ❖ strumenti di controllo, che rappresentano il "*come controllare*" e sono costituiti da:
  - organizzazione;
  - processi di pianificazione e controllo;
  - strumenti tecnico-contabili adottati per l'elaborazione delle informazioni;
  - sistemi informativi a supporto;
- ❖ timing, responsabilità di produzione, frequenza e destinatari.

- ***Sistema di Gestione della salute e sicurezza sul lavoro*** adottato ai sensi del D.lgs. n.81/2008 ed elaborato in base alle Linee Guida UNI-INAIL, meglio dettagliato nei pertinenti paragrafi della Parte Speciale L "Reati di salute e sicurezza in materia dei luoghi di lavoro";
- ***Sistema di Gestione della Qualità:*** l'attività svolta dalla società è, altresì, sottoposta a 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.

- ***Sistema di Gestione della Sicurezza delle Informazioni***: la politica di sicurezza delle informazioni in CY4gate ha l'obiettivo di proteggere le risorse informative da tutte le minacce, siano esse organizzative, tecnologiche, interne o esterne, accidentali o intenzionali, ponendosi i seguenti obiettivi aziendali:
  - garantire un adeguato livello di consapevolezza al personale, ai collaboratori e ai fornitori esterni;
  - mantenere allineato il Sistema Gestione Sicurezza Informazioni (SGSI) rispetto ai cambiamenti nelle procedure interne e nelle modalità di erogazione dei Servizi di CY4GATE;
  - garantire un adeguato governo dei fornitori al fine di assicurare il rispetto dei requisiti di sicurezza delle informazioni;
  - garantire un livello adeguato dei requisiti di riservatezza, integrità e disponibilità nei servizi erogati.

CY4gate ha ottenuto la certificazione ISO/IEC 27001:2013, che contraddistingue un preciso e dettagliato modo di operare dell'azienda, idoneo a fornire un prodotto ed un servizio di qualità relativamente alla sicurezza delle informazioni con riferimento ai seguenti settori:

- Progettazione, sviluppo, installazione, assistenza e manutenzione di sistemi HW e SW nel settore della Cybersecurity e Cyber Intelligence;
- Progettazione ed erogazione di servizi di consulenza specialistici per la Cyber Security di tipo MSS (managed security services);
- Network security; monitoraggio dei sistemi di sicurezza: VA/PT; SOC Management; Incident management & Analysis; Security advisory.

Una descrizione meglio dettagliata del sistema è disponibile nei pertinenti paragrafi della Parte Speciale B "Reati Informatici".

2.9. Piani di Audit

CY4gate, in particolare, conduce ad intervalli pianificati *audit* interni, sui sistemi precedentemente descritti, 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 e infine, (iii) al mantenimento del Sistema di Gestione relativo alla norma ISO/IEC 27001:2013.

Le verifiche sono condotte, per quanto concerne il punto (i) dalla società di revisione come da piano di revisione, e dal Collegio sindacale con cadenza trimestrale ed in occasione dell'approvazione del bilancio; per quanto concerne i punti (ii) e (iii) dall'Ente di certificazione dei Sistemi con cadenza annuale per il mantenimento della certificazione attraverso audit di sorveglianza e con cadenza triennale per i rinnovi.

I risultati degli Audit inerenti al sistema Qualità e Sicurezza delle informazioni sono registrati e archiviati sul portale dell'ente certificatore e, conseguentemente, sull'intranet aziendale CY4gate.

Infine, il Set-up della funzione IA prevede un piano in 4 steps:

1- Universo di Audit: definizione dell'Universo di Audit (i.e., insieme delle unità auditabili potenzialmente oggetto di attività di Internal audit) con raccolta e analisi documentale, esperienze di industry, hot topics della professione Internal audit
2- Prioritizzazione: definizione dei criteri (in prima applicazione, prevalentemente soggettivi) e prioritizzazione delle unità auditabili (driver strategici, rischi specifici);
3- Integrazione: revisioni interne ed integrazioni del piano di audit (confronto con Comitato CRS; discussiono con selezionato Top Management per la raccolta dei management concerns;
4- Piano di Audit 2023-2024: predisposizione della proposta di Piano di Audit 2023-2024 (con evidenza delle tipologie di intervento; degli obbiettivi e rischi; degli effort associati; della tempificazione).

2.10. Altre certificazioni/abilitazioni

a) 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 società, Associazione, persona, ecc. che fornisca servizi alle AD dei Paesi che aderiscono al NCS (Nato Codification System).

b) la Società 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.
c) La Società, è, altresì, registrata al Registro Nazionale delle Imprese e Consorzi di Imprese per esportazione, importazione transito ed intermediazione di materiali d'armamento in tutto o in parte, in alcune categorie, come meglio definite dal Decreto Ministeriale del 29 settembre 2021 (Gazzetta ufficiale del 9 ottobre 2021, n.242).
d) La Società è in possesso del NOSI (nulla osta sicurezza industriale) per la sede in Roma, via Coponia, 8.
e) Inoltre, la Società mantiene aggiornato il registro dei dipendenti a chi è stato rilasciato il NOS (nulla osta di sicurezza) e che hanno necessità di trattare informazioni con classifica di segretezza superiore a "riservato" nell'ambito di alcuni progetti.
f) Infine, CY4gate è certificata con il Label "Cybersecutity Made-In Europe".

2.11. Presupposti del Modello

Nella predisposizione del Modello, CY4gate ha tenuto conto del proprio sistema di controllo interno di gestione dei rischi nonché dei sistemi di controllo dei rischi più specifici gestiti attraverso i sistemi di controllo di gestione, della salute e sicurezza sul lavoro, della qualità e della sicurezza delle informazioni, 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, la definizione di un adeguato SCIGR, orientato a garantire, con ragionevole certezza, il raggiungimento di obiettivi operativi, di informazione e di conformità, permette di:

- identificare i rischi che possono incidere sul perseguimento degli obiettivi definiti dal Consiglio di Amministrazione;
- favorire l'assunzione di decisioni consapevoli e coerenti con gli obiettivi aziendali, nell'ambito di una conoscenza diffusa dei rischi e del livello di tolleranza agli stessi, della legalità e dei valori aziendali;
- salvaguardare il patrimonio aziendale, l'efficienza e l'efficacia dei processi, l'affidabilità dell'informazione fornita agli organi sociali e al mercato e il rispetto delle norme interne ed esterne.

Il SCIGR di CY4gate si ispira ai seguenti principi:

- integrazione del SCIGR nel generale assetto organizzativo di governo societario, amministrativo e contabile;
- direzione e coordinamento di CY4gate in qualità di capogruppo nei confronti delle società controllate;
- 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'OdV.

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.

2.12. Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali sviluppati da 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 il proprio SCIGR nonché gli standard ISO certificabili per i sistemi di gestione dei rischi specifici quali sulla qualità e la sicurezza delle informazioni;
- 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".

2.13. Parti speciali e 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.

Codice Etico

Nel Codice Etico (**All.2**) 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 e attuazione del Modello

In una logica di miglioramento continuo, il Modello 231 di CY4gate è soggetto ad aggiornamenti in occasione:

- delle novità e/o evoluzioni con riferimento (i) alla disciplina della responsabilità degli enti per gli illeciti amministrativi dipendenti da reato, ivi inclusi nuovi ambiti di applicazione del Decreto 231, (ii) al quadro normativo nelle materie di interesse e dei principi espressi da ulteriori normative di riferimento, (iii) alla giurisprudenza e alla dottrina in materia, nonché (iv) alla prassi delle società italiane ed estere in ordine ai modelli di compliance;
- dei cambiamenti significativi della struttura organizzativa o dei settori di attività di CY4gate;
- delle considerazioni derivanti dall'applicazione del Modello 231, ivi comprese le esperienze provenienti dal contenzioso penale.

È cura del CdA provvedere all'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'organo amministrativo si avvale del supporto dell'Organismo di Vigilanza.

Il CdA delega le singole strutture a dare attuazione ai contenuti del Modello e a curare il costante aggiornamento e l'implementazione della normativa interna e dei processi aziendali, che costituiscono parte integrante del Modello, nel rispetto dei principi di controllo e di comportamento definiti in relazione ad ogni attività sensibile.

L'efficace e concreta attuazione del Modello è garantita altresì:

- dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle singole unità organizzative nelle aree sensibili;
- dai responsabili delle varie unità organizzative in relazione alle attività a rischio dalle stesse svolte.

Il CdA deve inoltre garantire, anche attraverso l'intervento dell'Organismo di Vigilanza, l'aggiornamento delle aree sensibili e del Modello, in relazione alle esigenze di adeguamento che si rendono necessarie.

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 CdA, 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.

Tutte le modifiche e le integrazioni di cui sopra saranno tempestivamente comunicate ai Destinatari.

2.15. Modelli delle Società appartenenti al Gruppo

La Società CY4gate riveste la funzione di Capogruppo nei confronti di tutte le entità di cui detiene almeno la maggioranza societaria ed esercita la funzione di Direzione e coordinamento (Gruppo). L'attività di direzione e coordinamento è esercitata attraverso il controllo strategico, l'emanazione di direttive e regolamenti di gruppo ed attraverso funzioni operative di gruppo che assicurano omogeneità di gestione e l'integrazione di prodotto e di processo.

Il Gruppo CY4gate, a seguito delle recenti acquisizioni, ha avviato un progetto di integrazione del proprio sistema di controllo e di gestione al fine di attivare un costante monitoraggio delle performance aziendali ed il raggiungimento degli obiettivi del business, nonché di indirizzamento del SCIGR, che si applica a tutte le società del Gruppo con lo scopo di:

- fornire gli elementi d'indirizzo ai diversi attori del SCIGR, in modo da assicurare che i principali rischi, compresi quelli di sostenibilità nel medio-lungo periodo, risultino correttamente identificati e adeguatamente misurati, gestiti e monitorati;
- identificare i principi e le responsabilità di governo, gestione e monitoraggio dei rischi connessi alle attività aziendali;
- prevedere attività di controllo a ogni livello operativo e individuare con chiarezza compiti e responsabilità, in modo da evitare eventuali duplicazioni di attività e assicurare il coordinamento tra i principali soggetti coinvolti nel SCIGR.

Ferma restando l'autonoma responsabilità di ciascuna società appartenente al Gruppo in ordine all'adozione e all'efficace attuazione di un proprio "Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231", CY4gate, nell'esercizio della sua peculiare funzione di Capogruppo ha il potere di impartire criteri e direttive di carattere generale e di verificare mediante le funzioni Group Accouning, Finance, Controlling and Procurement, Group Human Resources, Legal & Shared Services, Internal audit, ciascuna per quanto di rispettiva competenza, la rispondenza dei Modelli delle società appartenenti al Gruppo a tali criteri e direttive.

Allo scopo di uniformare a livello di Gruppo le modalità attraverso cui recepire e attuare i contenuti del Decreto le società di cui CY4gate detiene la maggioranza devono attenersi

ai princìpi e ai contenuti del Modello della Capogruppo salvo che sussistano situazioni specifiche relative alla natura, dimensione o al tipo di attività esercitata nonché alla struttura societaria, all'organizzazione e/o all'articolazione delle deleghe interne che impongano o suggeriscano l'adozione di misure differenti al fine di perseguire più efficacemente gli obiettivi del Modello, nel rispetto comunque dei predetti principi nonché di quelli espressi nel Codice Etico.

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 (O.d.V.) 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

La nuova disciplina del "*whistleblowing*" ai sensi del D.Lgs. 24/2023 è intervenuta sull'articolo 6 comma 2bis stabilendo che i modelli organizzativi devono prevedere i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare.

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:

- Segnalazione mediante piattaforma web

Il segnalante visita la pagina web di **Integrity Line**, raggiungibile mediante collegamento dal sito Internet della società o all'indirizzo CY4GATE Group | Home (integrityline.com), inserisce un messaggio (in lingua italiana o inglese) e riceve un numero univoco identificativo della segnalazione. Il sistema deposita una copia del messaggio in uno spazio digitale accessibile dalla funzione legale della società e dai componenti dell'Organismo di Vigilanza, i quali la gestiranno in conformità allo strumento normativo aziendale in materia di segnalazioni.

Il segnalante ha, inoltre, la possibilità di registrare un messaggio vocale, caricare i documenti o scattare una foto, a supporto della segnalazione.

- Segnalazione in forma verbale, scritta o cartacea

Il segnalante deposita la comunicazione, redatta in forma cartacea secondo i princìpi contenuti nella procedura interna, nella cassetta a ciò dedicata sita presso la sede della società e contrassegnata con la dicitura "Segnalazioni interne".

Nell’ambito del Modello 231 le segnalazioni vanno indirizzate all’Organismo di Vigilanza tramite:

- comunicazione verbale all’ Organismo di Vigilanza;
- posta elettronica: OdV231@cy4gate.com disponibile anche nella rubrica aziendale;
- posta tradizionale via Coponia 8, 00131 Roma, Italia.

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:

- 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:

- le sue generalità;
- 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.

(c) Gestione delle segnalazioni

I principi di riferimento che orientano la gestione delle segnalazioni sono quelli posti dal D.Lgs. 24/2023 nonché dalle Linee Guida dell'ANAC e successivi aggiornamenti, tra cui:

- Garanzia di riservatezza e tutela del segnalante: l'Organismo di Vigilanza agirà in modo da assicurare l'assoluta riservatezza e la non divulgazione del nominativo delle persone segnalanti.
- Segnalazioni in mala fede: l'OdV. garantisce adeguata protezione dalle segnalazioni in mala fede e/o prive di fondamento, censurando simili condotte e informando di tali casi i soggetti/società interessati, come previsto dai principi generali del sistema sanzionatorio

- Requisiti di sicurezza e integrità dei dati: l'OdV. e la Società agiscono in modo da assicurare che i canali e le modalità di gestione delle segnalazioni garantiscano il rispetto dei requisiti di riservatezza, integrità e disponibilità dei dati attraverso le misure di sicurezza in essere per gli strumenti informatici aziendali.

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 comunicazione verso il personale nonché la formazione sui contenuti del Decreto e sull'attuazione del Modello, dandone evidenza all' OdV.

In tale contesto, le azioni comunicative prevedono:

- la comunicazione del Modello, del Codice Etico a tutti i dipendenti;
- 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.

Inoltre, CY4gate organizza specifici corsi destinati al personale che opera nelle aree sensibili con lo scopo di chiarire in dettaglio le criticità, i segnali premonitori di anomalie o irregolarità, le azioni correttive da implementare per le operazioni anomale o a rischio.

4.2 Informativa a Collaboratori Esterni, Consulenti e Partner

CY4gate promuove la conoscenza e l'osservanza del Modello e 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

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 (CCNL settore metalmeccanico industria), 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 settore metalmeccanico 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 3 ore della normale retribuzione calcolata sul minimo tabellare;
- sospensione dalla retribuzione e dal servizio fino ad un massimo di 3 giorni;
- 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 dal CCNL applicabile, 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'OdV 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'OdV.

In caso di violazioni del presente Modello da parte di uno o più componenti dell'OdV, gli altri componenti dell'OdV 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' OdV Egli dà, ugualmente,

notizia all'OdV 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.

SEZIONE SESTA

SEGNALAZIONE DELLE VIOLAZIONI (WHISTLEBLOWING)

6.1 Normativa applicabile

CY4gate attua la disciplina delle segnalazioni di c.d. *whistleblowing*, ai sensi del D.Lgs. 24/2023, anche nei confronti delle società del Gruppo, attraverso la gestione di canali dedicati.

La nuova disciplina del "*whistleblowing*", intervenuta sull'articolo 6 comma 2bis, stabilisce che i modelli organizzativi devono prevedere i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare.

6.2 Il segnalante

In applicazione del D.Lgs. 24/2023, il segnalante è la persona che segnala, divulga ovvero denuncia all'Autorità giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato.

Sono legittimate a segnalare le persone che operano nel contesto lavorativo di un soggetto del settore pubblico o privato, in qualità di:

- dipendenti pubblici;
- lavoratori subordinati di soggetti del settore privato;
- lavoratori autonomi che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;
- collaboratori, liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- volontari e i tirocinanti, retribuiti e non retribuiti;

- azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato.

6.3 Quando e cosa segnalare

Quando si può segnalare:

- quando il rapporto giuridico è in corso;
- durante il periodo di prova;
- quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso (pensionati).

Cosa si può segnalare:

Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

Violazioni di disposizioni normative nazionali:

- Illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231(reati presupposto) o violazioni dei modelli di organizzazione e gestione ivi previsti.

Violazioni di disposizioni normative europee:

- Illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea relativi ai seguenti settori:
    - appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radio protezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;

- Atti od omissioni che ledono gli interessi finanziari dell'Unione;
- Atti od omissioni riguardanti il mercato interno (a titolo esemplificativo: violazioni in materia di concorrenza e di aiuti di Stato);
- Atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

6.4 I canali di segnalazione

Le segnalazioni devono essere trasmesse attraverso canali appositamente predisposti:

- Canale Interno;
- Canale Esterno (A.N.AC);
- Divulgazioni pubbliche;
- Denuncia all'Autorità giudiziaria.

Conviene precisare che la scelta del canale di segnalazione non è più rimessa alla discrezione del segnalante in quanto in via prioritaria è favorito l'utilizzo del canale interno e, solo al ricorrere di una delle condizioni di cui all'art. 6 del D.lgs. 24/2023, è possibile effettuare una segnalazione esterna.

CY4gate ha attivato **due canali interni** per la trasmissione e la gestione delle segnalazioni che garantiscano la riservatezza della persona segnalante, del facilitatore, della persona coinvolta o comunque dei soggetti menzionati nella segnalazione nonché del contenuto della segnalazione e relativa documentazione.

I canali di segnalazione sono descritti all'articolo 7 del regolamento dell'OdV (Sezione Terza).

6.5 Tutela del segnalante e gestione delle segnalazioni "231"

I principi di riferimento che orientano la gestione delle segnalazioni sono quelli posti dal D.Lgs. 24/2023 nonché dalle Linee Guida dell'ANAC e successivi aggiornamenti, come meglio elencati e descritti all'articolo 7 del regolamento dell'ODV (Sezione Terza). Si precisa, inoltre, che viene garantito il:

- Divieto di ritorsione: in nessun caso la Società può applicare al segnalante in buona fede qualsiasi forma di ritorsione o minaccia per effetto della segnalazione quali, a titolo esemplificativo, licenziamento, mancata promozione, demansionamento, riduzione della retribuzione, discriminazione o mancato rinnovo del contratto di lavoro.

ALLEGATI

Allegato 1: Elenco e descrizione dei reati-presupposto ex. D.Lgs 231/01

Allegato 2: Codice Etico

Allegato 3: Codice anticorruzione

Allegato 4: Policy per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo