

MODELLO DI ORGANIZZAZIONE E CONTROLLO

Parte Generale

ex Decreto Legislativo 8 giugno 2001 n. 231

Agg.to Febbraio 2025

Cyber-Bee S.r.l.

**SEDE LEGALE
E DIREZIONE CENTRALE**
00166 Roma Via Monte Carmelo, 5

SEDE DI MILANO
20134 Milano Via Cavriana, 14

SEDE DI PERUGIA
06128 Perugia Via Pietro Tuzi, 11

SEDE DI NAPOLI
80143 Napoli Centro Direzionale
Is. E/5 sc.A

CAPITALE SOCIALE € 100.000,00 i.v. R.E.A. di Roma n 1529928 Cod. Fisc. E P. IVA

cyber-bee.it

Sommario

SEZIONE PRIMA	3
1. IL DECRETO LEGISLATIVO 231/2001	3
1.1. La responsabilità amministrativa degli Enti	3
1.2. I reati previsti dal Decreto	4
1.3. Le sanzioni previste dal Decreto	4
1.4. Condizione esimente della responsabilità amministrativa	5
1.5. Le “Linee Guida” di Confindustria	6
1.6. Delitti tentati e delitti commessi all'estero	8
SEZIONE SECONDA	9
2. IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO DI CYBER-BEE SRL	9
2.1. Obiettivi e mission aziendale	9
2.2. Modello di Governance	10
2.3. Finalità del Modello	12
2.4. Destinatari	13
2.5. Struttura del Modello	13
2.6. Elementi fondamentali del Modello	14
2.7. Codice Etico e Modello	15
2.8. Presupposti del Modello	15
2.9. Adozione e gestione del Modello nell’ambito di Cyber-Bee srl	15
2.10. Individuazione delle attività “a rischio”	16
2.11. Principi di controllo interno generali	16
SEZIONE TERZA	19
3. ORGANISMO DI VIGILANZA	19
3.1. Funzioni e poteri dell’Organismo di Vigilanza	19
3.2. Reporting dell’Organismo di Vigilanza	20
3.3. Flussi informativi nei confronti dell’Organismo di Vigilanza	20
SEZIONE QUARTA	23
4. SISTEMA DISCIPLINARE	23
5. AGGIORNAMENTO DEL MODELLO	23
6. INFORMAZIONE E DIFFUSIONE DEL MODELLO TRA I PORTATORI D’INTERESSE	23



SEZIONE PRIMA

1. IL DECRETO LEGISLATIVO 231/2001

1.1. La responsabilità amministrativa degli Enti

Il Decreto Legislativo 8 giugno 2001, n. 231 disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (enti). La innovazione legislativa (rivoluzionaria del principio *societas puniri non potest*) non stravolge i confini di liceità delle azioni degli enti: introduce, per la prima volta nell'ordinamento giuridico italiano, sanzioni amministrative di natura penale per Enti colpevoli -anche con dolo eventuale- di reati ascritti sempre a condotte poste in essere da persone fisiche. Discolpa l'azione delittuosa verso l'Ente che sia in grado di dare prova che delitti/reati non hanno ragionevolmente comportato un interesse e/o un vantaggio dell'Ente stesso.

La disciplina degli affari virtuosi è parte dell'ordinamento giuridico italiano e ne impronta la stessa genetica della autonomia contrattuale delle parti, pubbliche e private. Le Leggi italiane sono perfettamente rispondenti alle Convenzioni internazionali cui l'Italia ha già da tempo aderito, e che consentono al nostro Paese di esser soggetto dignitario del Mondo che combatte gli affari illeciti. Sono nostre condivise regole, quelle ad esempio particolari convenute ne:

- 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 nella quale sono coinvolti 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;

che prevedono paradigmi di responsabilità delle persone giuridiche e un corrispondente sistema disciplinare che colpisce la criminalità d'impresa.

La responsabilità amministrativa deriva innanzitutto da un reato commesso nell'interesse dell'ente; il rigore della regola va oltre anche il singolo prospetto sanzionato della condotta illecita che sia posta in essere con l'intento di arrecare un beneficio/vantaggio alla società. Il divieto non si infrange neanche in caso di vantaggio indiretto, cioè quando l'autore del reato abbia agito senza il fine di recare un beneficio alla società. E pertanto, il solo vantaggio esclusivo dell'agente (o di un terzo rispetto all'ente) esclude la responsabilità dell'ente, versandosi in una situazione di assoluta e manifesta estraneità dell'ente al fatto di reato. Sicché alla Società è imposto di dar prova di aver fatto di tutto per escludere che abbia tratto un qualche interesse nella condotta del responsabile del delitto.

La responsabilità degli enti si estende anche ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto, sempre che sussistano le particolari condizioni previste dal D.lgs. 231/2001.

In particolare, gli Enti diventano responsabili per alcune fattispecie di reato se questi sono compiuti da:

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

La responsabilità amministrativa degli Enti non si sostituisce a quella della persona fisica che ha materialmente commesso il reato (ovviamente tutti gli atti delle persone giuridiche si estrinsecano per l'operato di persone fisiche) ma si cumula con quella e sono entrambe accertate nel corso del medesimo procedimento innanzi al giudice penale. Se l'autore materiale del reato rimane ignoto (o comunque risulti essere non punibile) la responsabilità dell'Ente comunque non si estingue.



1.2. I reati previsti dal Decreto

I reati dal cui compimento è fatta derivare la responsabilità amministrativa dell'ente, sono quelli espressamente e tassativamente richiamati dal Decreto e successive modifiche ed integrazioni.

Nel documento "Appendice 1 – Reati ed Illeciti", sono esposte le varie tipologie di Reati ed Illeciti previste dal D. Lgs. N. 231/2001.

1.3. Le sanzioni previste dal Decreto

Il sistema sanzionatorio, a fronte del compimento dei reati sopra elencati, prevede l'applicazione delle seguenti sanzioni amministrative:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca (del prezzo o del profitto del reato);
- pubblicazione della sentenza.

La sanzione pecuniaria è ridotta nel caso in cui:

- a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio (permanendone l'interesse aziendale) o ne ha ricavato un vantaggio minimo;
- b) il danno patrimoniale cagionato è di particolare tenuità, o se, prima della dichiarazione di apertura del dibattimento in primo grado:
 - l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso e,
 - un Modello è stato adottato e reso operativo.

Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni:

- a) l'Ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti che ricoprono una posizione di rappresentanza, amministrativa o gestoria nell'Ente ovvero da soggetti sottoposti alla direzione o al controllo dei primi e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; o
- b) in caso di reiterazione degli illeciti.

Il Decreto prevede le seguenti sanzioni interdittive che possono avere una durata non inferiore a tre mesi e non superiore a due anni:

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

Ai sensi della vigente normativa, le sanzioni interdittive non si applicano in caso di commissione dei reati societari, di *market abuse* e di induzione a non rendere o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

Il Decreto prevede, inoltre, che, qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione interdittiva, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

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



1.4. Condizione esimente della responsabilità amministrativa.

Il Modello di Organizzazione, Gestione e Controllo è uno strumento di gestione del rischio specifico di realizzazione di determinati reati.

Il D.lgs. 231/2001 espressamente prevede, agli artt. 6 e 7, l'esenzione dalla responsabilità amministrativa qualora l'ente si sia dotato di effettivi ed efficaci "Modelli di organizzazione e di gestione" idonei a prevenire i reati previsti nel decreto: l'adeguata organizzazione rappresenta pertanto il solo strumento in grado di escludere la "colpa" dell'ente e, conseguentemente, di impedire l'applicazione delle sanzioni a suo carico.

Segnatamente, la responsabilità è esclusa se l'ente prova che:

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

L'adozione del modello costituisce dunque la misura della diligenza definita dal legislatore e rappresenta per l'ente la possibilità di esimersi dalla propria responsabilità.

Tuttavia, la mera adozione del Modello da parte dell'organo dirigente – da individuarsi nell'Ufficio di gestione amministrativa – non è tuttavia misura sufficiente a determinare l'esonero da responsabilità dell'ente, essendo piuttosto necessario che il Modello sia anche **efficace** ed **effettivo**.

Quanto all'**efficacia** del Modello, il legislatore, all'art. 6 comma 2 D.lgs. 231/2001, statuisce che il Modello deve soddisfare le seguenti esigenze:

- a) individuare le attività nel cui ambito possono essere commessi reati (cosiddetta "mappatura" delle attività a rischio);
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli.

La caratteristica dell'**effettività** del Modello è invece legata alla sua efficace attuazione che, a norma dell'art. 7 comma 4 D. Lgs. 231/2001, richiede:

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

Per questa duplice finalità, Cyber-Bee srl ha scelto di assommare ai poteri di vigilanza e controllo conferiti al proprio Organismo, anche funzioni di Garante del Codice Etico.

Le scelte d'adozione del Modello e dei vincoli che l'Organismo di Vigilanza impone a Cyber-Bee srl sono espressione della determinazione aziendale che è stata rivolta alle regolamentazioni di categoria ed a quelle che, anche la prassi inveterata, sono risultate più efficaci e di pronto adempimento alle disposizioni legislative. Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni



rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sull'idoneità del Modello a prevenire i reati. Con riferimento ai reati ed illeciti amministrativi in materia di *market abuse*, tale valutazione di idoneità viene compiuta dal Ministero della Giustizia, sentita la Consob.

In merito alla reale applicazione del Modello, il Decreto impone:

- una verifica periodica, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal Modello o intervengano mutamenti nell'organizzazione o nell'attività dell'ente ovvero modifiche legislative, la modifica del Modello (cfr. par. 5 – “Aggiornamento del Modello”);
- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello.

1.5. Le “Linee Guida” di Confindustria

Per espressa previsione legislativa (art. 6, comma 3, D.lgs. 231/2001), i Modelli di organizzazione e di gestione possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia.

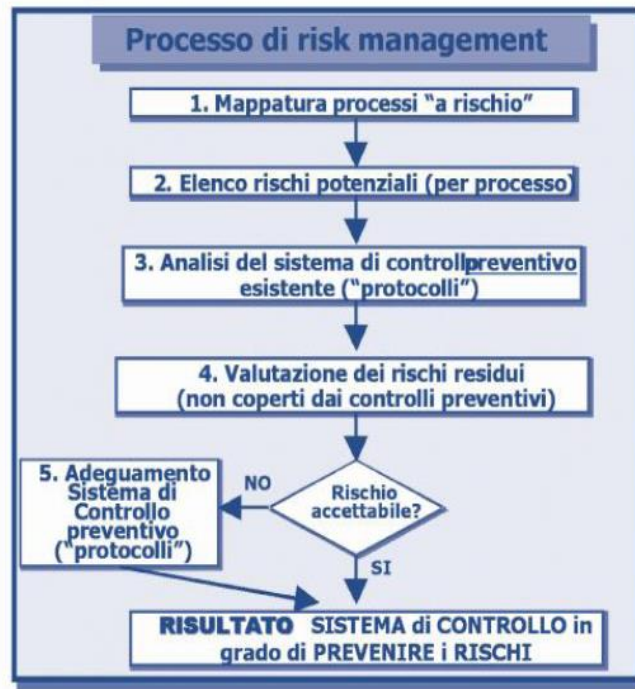
Benché Cyber-Bee srl non sia iscritta ad alcuna Associazione di categoria imprenditoriale, essa stessa ha scelto di condurre la disciplina del proprio Codice Etico coniugando le indicazioni offerte da Confindustria, in data 23 luglio 2014; ed in particolare con la versione aggiornata delle “Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex D.lgs. 231/01” che ha emanato la Associazione stessa. Il Ministero di Grazia e Giustizia ha approvato dette Linee Guida, ritenendo che l'aggiornamento effettuato sia da considerarsi “complessivamente adeguato ed idoneo al raggiungimento dello scopo fissato dall'art. 6 del Decreto”.

Le linee guida di Confindustria sono dunque le Linee Guida di R1 Group; sono regole che indicano un percorso che può essere in sintesi così riepilogato e che Cyber-Bee srl ha fatto proprio:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare i reati previsti dal Decreto;
- la predisposizione di un sistema di controllo¹ (i c.d. protocolli) idoneo a prevenire i rischi di reato identificati nella fase precedente, attraverso la valutazione del sistema di controllo esistente all'interno dell'ente ed il suo grado di adeguamento alle esigenze espresse dal Decreto.

¹ Il sistema di controllo esistente all'interno dell'ente, o sistema di controllo interno, “è l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati” (v. Codice di Autodisciplina, Comitato per la Corporate Governance, Borsa Italiana S.p.A., 2006, pag. 35).





2

Le componenti più rilevanti del sistema di controllo ideato da Confindustria sono:

- la individuazione di principi etici e di regole comportamentali tradotte in un codice di condotta (Codice Etico);
- un Organigramma ben definito con relativo mansionario e responsabilità attribuite;
- procedure, manuali e/o informatiche, che disciplinino lo svolgimento delle attività, prevedendo opportuni controlli;
- poteri autorizzativi e di firma coerenti con quanto delineato dal mansionario stabilendo, se necessario, limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

Cyber-Bee srl ha attuato il Sistema di Controlli suggerito da Confindustria e se ne avvale per ridurre i rischi di condotte illecite e per prevenirne di simili.

Per questo, le componenti del Sistema di Controlli di Cyber-Bee srl sono informate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli effettuati;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- individuazione dell'Organismo di Vigilanza, dotato dei requisiti di autonomia e indipendenza, professionalità e continuità di azione, quale soggetto designato da Cyber-Bee srl al quale le varie funzioni aziendali debbono inviare una serie di informazioni utili al controllo e vigilanza per la prevenzione delle condotte che possano commettere reati.

Per la predisposizione del proprio Modello di organizzazione e gestione, Cyber-Bee srl ha quindi espressamente tenuto conto:

- delle disposizioni del D.lgs. 231/2001, della relazione ministeriale accompagnatoria e del decreto ministeriale 26 giugno 2003 n. 201 recante il regolamento di esecuzione del D.lgs. 231/2001;
- della versione ultima delle Linee guida predisposte da Confindustria.

² Schema tratto dalle "Linee Guide di Confindustria per la costruzione del Modello di Organizzazione, gestione e controllo ai sensi del D.Lgs 231/2001"

1.6. Delitti tentati e delitti commessi all'estero

L'Ente risponde anche degli illeciti dipendenti da delitti tentati e da reati commessi all'estero.

Nelle ipotesi di commissione nella forma del tentativo dei delitti previsti dal Decreto, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto.

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere, in relazione a reati – contemplati dallo stesso Decreto – commessi all'estero, al fine di non lasciare sfornita di sanzione una condotta criminosa di frequente verifica, nonché al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

I presupposti su cui si fonda la responsabilità dell'Ente per reati commessi all'estero sono:

- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;
- l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
- le condizioni previste dagli artt. 7, 8, 9, 10 Codice penale, con riferimento alla punibilità dei reati commessi all'estero, si devono essere verificate (nell'Allegato B – “Articoli del Codice penale richiamati dall'art. 4 del D.lgs. 231/2001”, sono descritte le fattispecie dei reati);
- non si procede nei confronti dell'Ente nello Stato in cui è stato commesso il fatto.



SEZIONE SECONDA

2. IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO DI CYBER-BEE SRL

2.1. Obiettivi e mission aziendale

Cyber-Bee srl, avente sede legale e amministrativa in Italia, offre servizi e consulenze in ambito sicurezza delle aziende, al fine di individuare eventuali vulnerabilità dell'infrastruttura e delle applicazioni aziendali e minimizzare il volume ed il peso degli incidenti di sicurezza informatica e Cybersecurity.

- **Project Management**

il Project Management è inteso come la copertura totale di un progetto: inizia con il fornire supporto alla struttura di vendita nell'analizzare, progettare, disegnare e proporre una soluzione, e prosegue fino alla consegna che si completa con il collaudo; passaggi obbligati sono la pianificazione, la programmazione, la prototipizzazione e quindi la realizzazione, l'implementazione e l'inserimento in produzione, anche (e preferibilmente) su aree tecnologiche diversificate (offering) e con elevato livello di complessità.

- **Virtualizzazione**

Soluzione dedicata alle aziende che cercano la flessibilità in un'ottica di ottimizzazione di costi e di risorse. Le tecnologie di virtualizzazione consentono di ottimizzare le risorse, semplificare la mobilità e la gestione, nonché migliorare la adattabilità sull'intera infrastruttura IT.

- **Networking**

Cyber-Bee è in possesso di know-how in grado progettare e offrire soluzioni di networking alle grandi e alle piccole/medie aziende per la creazione di reti Cablate e Wireless che siano efficienti ed affidabili. Inoltre, essa è in grado di offrire soluzioni VoIP, gestione della rete e cablaggio strutturato.

- **Gestione Documentale**

La gestione documentale permette di conservare i documenti elettronicamente e di gestirli dalla loro creazione fino alla consultazione. L'orientamento verso una gestione documentale informatizzata consente alle aziende di ottenere vantaggi immediati: organizzazione dei propri documenti in modo logico, velocità di ricerca, ottimizzazione dei costi legati alla carta e alla stampa dei documenti, riduzione degli spazi fisici, consultazione veloce ed ottimizzata.

- **Hardware e Software per l'Infrastruttura**

Cyber-Bee basa anche il proprio business sulla proposizione di hardware e software. Per affrontare la competitività che contraddistingue questo tipo di attività, l'Azienda si è strutturata e distinta per alcune caratteristiche indispensabili: per poter vendere a volume è necessaria una buona solidità finanziaria, proporsi con prodotti innovativi, far fronte velocemente alle richieste del cliente e, naturalmente, seguire processi aziendali che siano snelli, sperimentati e certificati. Fornire consulenza e supporto ai clienti per la pianificazione e acquisizione delle opzioni di licensing per le tecnologie dei migliori software vendor.

- **Sicurezza**

Nell'information Technology moderna un ruolo rilevante è ricoperto dalla sicurezza. Una definizione classica di sicurezza cita: "la conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati". In altri termini è sapere



che quello che faremo non provocherà dei danni. Tale definizione trova una rilevanza molto ampia nell'ICT in quanto diventa sempre più importante riconoscere e prevenire ciò che provocherà danni. I rischi alla sicurezza, con l'esplosione delle comunicazioni web, oggi non provengono solo dall'esterno ma anche e forse soprattutto dall'interno. Per questo motivo, grazie alle tecnologie sviluppate da molti Brand, è possibile posizionare degli strumenti perimetrali di filtro che impediscono l'ingresso e l'uscita di tutto ciò che, all'interno di una azienda, viene definito "a rischio". Gli strumenti di sicurezza perimetrale offrono il valore aggiunto ai classici strumenti di protezione delle postazioni di lavoro e dei server. Altro elemento fondamentale nella valutazione di rischio, e quindi di sicurezza, è quello relativo alle informazioni. La produttività e la competitività di una azienda è data dalle informazioni residenti al suo interno. Anche per questo diventa importante impedirne l'utilizzo improprio. In aiuto del business concorrono quegli strumenti che attraverso l'uso di politiche procedurali e metodologiche ne impediscono la compromissione in tutte le sue eccezioni.

2.2. Modello di Governance

L'attuale sistema di governo societario di Cyber-Bee si basa sulla presenza di un Amministratore Unico, che ha la rappresentanza generale della Società nei confronti dei terzi per il compimento degli atti che rientrano nell'oggetto sociale. All'Amministratore Unico competono tutti i poteri per la gestione ordinaria e straordinaria della Società.

Cyber-Bee è parte di R1 Group, un gruppo societario che si compone delle seguenti società:

- R1 S.p.A. (c.d. "Controllante"), società che detiene le quote di maggioranza di tutte le altre società del Gruppo e delinea un indirizzo, indicando principi comuni a livello di Codice Etico condivisi da tutte le società controllate (si veda elenco seguente);
- Eurome s.r.l. (società controllata da R1 S.p.A.);
- Gway s.r.l. (società controllata R1 S.p.A.);
- R1 Lease s.r.l. (società controllata R1 S.p.A.);
- Cyber Bee s.r.l. (società controllata R1 S.p.A.);
- Trice s.r.l. (società controllata R1 S.p.A.).

I rapporti tra la Controllante e le Controllate sono definiti da specifici contratti di servizio, volti a definire i meccanismi con cui le società stesse si rapportano tra di loro nell'ambito dei servizi intercompany.

In merito alla struttura organizzativa di Cyber-Bee, per il cui dettaglio si rimanda all'organigramma aziendale, alcune attività di supporto amministrativo e organizzativo (funzioni di staff) sono affidate alla Controllante. Tale struttura organizzativa è stata progettata per rispondere al meglio alle esigenze di efficienza e riduzione costi richieste dal mercato.

In generale, Cyber-Bee adotta, attraverso l'operato dei suoi amministratori, proprie strategie di politica aziendale, seppur all'interno di un perimetro di indirizzo generale e di rispetto della legalità impresso dalla Controllante alle controllate.

Sistema delle deleghe interne

Vengono delegati all'Amministratore Unico poteri di rappresentanza legale della Società, poteri afferenti alla gestione del personale, poteri in ambito contrattuale e limiti di spesa, nonché poteri in materia contabile e di sicurezza sul lavoro. L'Amministratore Unico è identificato quale Datore di Lavoro ai sensi del D.Lgs. 81/2008.



Nell'ambito del proprio sistema di deleghe e procure, Cyber-Bee ha disciplinato le modalità di gestione delle risorse finanziarie in materia di spese relative "all'approvvigionamento di beni e servizi". L'esercizio delle deleghe è posto sotto controllo esistendo la tracciabilità di ogni singola operazione sulle risorse finanziarie.

Le attività affidate in outsourcing, sia all'interno del Gruppo che al di fuori dello stesso, sono formalizzate attraverso la stipula di specifici contratti che assicurano alla Società:

- l'assunzione di ogni decisione nel rispetto della propria autonomia, mantenendo la necessaria responsabilità su tutte le attività, ivi comprese quelle relative ai servizi esternalizzati;
- il rispetto delle politiche di indirizzo della Controllante.

Principi di indirizzo di Gruppo

Ferma restando l'autonoma responsabilità di Cyber-Bee in ordine all'adozione e all'efficace attuazione di un proprio Modello ai sensi del Decreto 231 nonché in ordine alla nomina dell'Organismo di Vigilanza, la Controllante impartisce criteri e direttive che sono il risultato dei principi etici e morali, nonché di rispetto della normativa condivisi dal Gruppo stesso: tali principi sono riflessi nel Codice Etico nonché nella Parte Generale del MOGC, documenti attualmente in condivisione tra tutte le società appartenenti al Gruppo.

Allo scopo di garantire omogeneità nel recepimento e attuazione dei contenuti della normativa 231, predisponendo presidi adeguati, sono di seguito delineati i principi di indirizzo definiti dalla Controllante R1 S.p.A., a cui tutte le società appartenenti al Gruppo devono attenersi, pur nel rispetto della propria autonomia giuridica:

- identificazione delle attività aziendali che presentano profili di rischio elevati e delle misure più idonee a prevenirne la realizzazione nella Parte Speciale del MOGC. Cyber-Bee deve attenersi ai principi e ai contenuti della Parte Generale salvo che sussistano situazioni specifiche 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;
- nomina dell'Organismo di Vigilanza;
- comunicazione dell'avvenuta nomina dell'OdV alla Direzione della Controllante;
- sistematico aggiornamento del Modello in funzione di modifiche normative e organizzative, nonché nel caso in cui significative e/o ripetute violazioni delle prescrizioni del Modello lo rendessero necessario;
- predisposizione di adeguate attività di formazione e di comunicazione per il personale, nonché interventi specifici di formazione destinati a figure impegnate in attività valutate come aventi elevata rischiosità.

La competenza e la responsabilità per l'approvazione e l'efficace attuazione del Modello restano in capo a Cyber-Bee.

Cyber-Bee si avvale di un OdV monocratico. Tra gli Organismi di Vigilanza delle varie società di R1 Group sono sviluppati rapporti informativi periodici, tali da garantire la completezza e tempestività delle notizie utili ai fini di attività ispettive da parte degli organi di controllo. Questi scambi hanno natura puramente informativa e sono attentamente disciplinati.

Cyber-Bee può ricorrere alla nomina a proprio OdV, qualora lo ritenga opportuno, di componenti dell'OdV della Controllante. Allo stesso modo, qualora per le attività ispettive e di verifica sia accertata l'impossibilità di esecuzione con risorse interne, Cyber-Bee potrà richiedere il supporto delle risorse della Controllante.

Nel modello di governance di Cyber-Bee, svolge un ruolo cruciale la funzione *Compliance*, che è parte integrante del sistema di controllo interno e di gestione dei rischi a livello di gruppo societario, basato su un modello di controlli integrato.



Essa si occupa di vigilare sul rispetto delle norme legali all'interno dell'azienda. Tra le sue responsabilità rientrano la gestione della responsabilità amministrativa degli enti, l'applicazione del Codice Etico, la prevenzione di illeciti come corruzione e riciclaggio, la conformità alle leggi antitrust, la tutela della privacy, la protezione dei consumatori e l'adeguamento alle regolamentazioni finanziarie. L'ufficio Compliance svolge diverse funzioni all'interno dell'azienda:

1. Monitora tutti i processi e le procedure operative, integrandole in un programma di gestione della compliance che garantisce il rispetto da parte dell'azienda di norme e standard etici;
2. Gestisce il flusso di informazioni ricercando, registrando e analizzando dati e attività. Con un flusso regolare di informazioni e valutando il rischio di compliance, assicura che le diverse attività aziendali si svolgano senza intoppi;
3. Forma e istruisce i dipendenti in modo che siano informati riguardo eventuali modifiche legali e aggiornati su modifiche delle linee guida di compliance. Mantenere il personale informato è essenziale per garantire la conformità.
4. Agisce come persona di contatto e collegamento tra i responsabili dei diversi dipartimenti e board management. Regola i flussi informativi tra i livelli più alti dell'azienda e le diverse aree specialistiche, nel rispetto delle responsabilità e dei requisiti di riservatezza;
5. Esegue valutazioni periodiche per verificare se le policy aziendali sono conformi alla legge.

L'ufficio Compliance è responsabile di garantire che l'azienda operi in modo etico, legale e conforme alle normative applicabili.

Si evidenzia che, al fine di rafforzare il Sistema di Controllo Interno, il **Consiglio di Amministrazione (CdA)** della Controllante R1 S.p.A. ha deliberato l'istituzione della funzione di **Internal Audit** in data 20/01/2025, riconoscendone il ruolo essenziale nel garantire l'efficacia del sistema di controllo attraverso una corretta gestione del rischio. L'Internal Audit, la cui competenza è estesa anche a tutte le società controllate da S.p.A., opera come funzione indipendente e obiettiva, con il compito di valutare l'adeguatezza e l'efficacia dei presidi di controllo adottati dall'azienda, individuare eventuali criticità e proporre azioni correttive finalizzate al miglioramento continuo dell'efficienza operativa e della governance aziendale.

Dal punto di vista organizzativo, l'Internal Audit è collocato in posizione di **staff al Consiglio di Amministrazione**, con rapporto diretto al CdA, a garanzia della sua autonomia e imparzialità. Questa configurazione assicura che le attività di audit vengano svolte in modo indipendente rispetto alle funzioni operative, consentendo di monitorare e verificare con obiettività i processi aziendali e la loro rispondenza ai principi di trasparenza nonché di proporre eventuali azioni correttive in caso di anomalie riscontrate.

2.3. Finalità del Modello

Il Modello ha come scopo quello di creare in primis una coscienza aziendale di legalità suffragata da adeguati strumenti operativi volti ad identificare le aree a rischio, codificare le procedure volte alla prevenzione e riduzione dei reati il tutto costantemente monitorato dall'Organismo di vigilanza che garantisce effettività nella individuazione dei comportamenti illeciti e del loro autore, comminando sanzioni e suggerendo le opportune modifiche alle procedure.

Richiamandoci allo schema precedentemente citato di Confindustria un Modello deve consentire di:

- individuare preliminarmente i "processi a rischio";
- analizzare i rischi che ne derivano;
- valutare l'efficacia dei controlli attuali in materia di prevenzione dei suddetti rischi;
- decidere se adeguare i controlli interni alla luce di quanto non eventualmente coperto (analizzare i rischi residui – determinarne i possibili oneri – confrontarli con i costi certi di adeguamento delle metodologie).

Il Modello di Cyber-Bee srl è quindi:

- **idoneo** allo scopo per cui è stato costruito (individuazione delle aree a rischio e prevenzione delle eventuali conseguenze negative);
- **specifico** per diretta conseguenza di quanto sopra scritto;
- **aggiornato** costantemente alla luce di tutte le novità che dovessero emergere e alle evoluzioni aziendali.



I principi della presente Parte Generale sono condivisi dalla società Controllante e dalle Controllate.

2.4. Destinatari

Le regole contenute nel Modello si applicano:

- a coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale, amministratore, direttore generale, membro del collegio sindacale;
- a coloro i quali svolgano funzioni di direzione in veste di responsabili di specifiche Unità Organizzative;
- a coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società. La previsione, di portata residuale, è finalizzata a conferire rilevanza al dato fattuale, in modo da ricomprendere, tra gli autori dei reati da cui può derivare la responsabilità della società, non soltanto l'amministratore di fatto (ovvero colui che esercita in concreto, senza averne la qualifica, poteri corrispondenti a quelli dell'amministratore), ma anche, ad esempio, il socio azionista di maggioranza, che sia in grado di imporre la propria strategia aziendale e il compimento di determinate operazioni, anche nell'ambito di una società controllata, comunque agendo, attraverso qualsiasi forma idonea di controllo, sulla gestione concreta della società;
- ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale, ancorché distaccati all'estero per lo svolgimento dell'attività;
- a chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima. Resta quindi inteso che eventuali risorse appartenenti alle Controllate, qualora operino, anche in territorio estero, per conto o nell'interesse della Società, devono intendersi come Destinatari del Modello e dovranno, pertanto, osservare le regole comportamentali ed i principi sanciti nel Modello di Cyber-Bee srl

Il Modello costituisce un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di materiali, servizi e lavori, consulenti, partners nelle associazioni temporanee o società con cui Cyber-Bee srl opera.

2.5. –Struttura del Modello

Il presente Modello è costituito da:

- Parte Generale che espone i principi di riferimento e le linee guida adottate da Cyber-Bee srl;
- Codice Etico di gruppo;
- Sistema Disciplinare;
- Risk Assessment dei processi aziendali rispetto alle categorie di reato;
- Appendice normativa che espone le varie tipologie di Reati ed Illeciti previste dal D.Lgs n. 231/2001;
- Parte Speciale che si riferisce alle tipologie di reato presupposto, identificate nell'ambito di un'attività di mappatura delle "Aree a rischio reato" e per le quali è stato ritenuto che Cyber-Bee sia, in via potenziale ed eventuale, esposta ad essere imputata di condotte illecite in considerazione delle attività svolte.

Sono altresì da considerarsi parte integrante del MOGC anche:

- il Sistema di gestione della Qualità redatto ed implementato secondo il dettato della norma UNI EN ISO 9001;



- il Sistema di Gestione della Sicurezza delle Informazioni redatto ed implementato secondo il dettato della norma standard ISO/IEC 27001;
- il Documento di Valutazione dei Rischi redatto ed implementato secondo il dettato del D.lgs. 81/08 per la fattispecie dei reati relativi alla sicurezza sul lavoro;
- le Linee Guida di Confindustria riferiti ai documenti CoSO;
- i documenti CoSO Report I, II, III (Committee of Sponsoring Organizations of the Treadway Commission);
- gli I.S.A. (International Standards on Auditing) riferiti al rischio di commissione di illeciti e reati;
- i principi di Pratica Professionale in materia di revisione contabile che a questi ultimi fanno riferimento e che soddisfano i requisiti richiesti dal CoSO Report I;
- la Legge n. 179 del 30 novembre 2017 («Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato») ovvero l'istituto del "whistleblowing".

Le Sources sopra indicate sono parte integrante del "Modello" che si concretizza in un articolato sistema piramidale di principi e procedure.

2.6. Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto e dalle linee guida di Confindustria, gli elementi fondamentali sviluppati da Cyber-Bee srl nella definizione del Modello, possono essere così riassunti:

- **identificazione** delle attività da cui potenzialmente possono derivare la commissione di reati dolosi o colposi e quindi da sottoporre a controlli continui;
- **adozione** di particolari protocolli e/o integrazione delle procedure aziendali interne per le aree di attività ritenute a maggior rischio potenziale di commissione di reato, idonei a disciplinare la concretizzazione delle decisioni sociali diretti a regolamentare espressamente la formazione e l'attuazione delle decisioni della Società, al fine di fornire indicazioni specifiche sul sistema di controlli preventivi in relazione alle singole fattispecie di illecito da prevenire. Nei protocolli sono inoltre contenute le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati stessi;
- **individuazione** dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal Decreto, sancite nel Codice di Condotta adottato dalla Società e, più in dettaglio, nel presente Modello;
- **nomina** 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, nonché compiti di Internal Audit raccolte le iniziative protette tramite la corretta presentazione e gestione delle segnalazioni di rischi e/o condotte;
- **approvazione** di un sistema disciplinare idoneo a dare effettività a quanto sopra stabilito;
- **svolgimento** di un'attività di informazione, sensibilizzazione e divulgazione ai Destinatari del presente Modello;
- **modalità** per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso.



2.7. Codice Etico e Modello

Il Codice Etico di R1 Group è un'enunciazione di Principi e Regole che l'Azienda riconosce come propri e che costituiscono le fondamenta per la definizione dei comportamenti operativi.

Cyber-Bee srl, attraverso tale documento, intende fissare e far rispettare le regole di condotta cui la Società si attiene nelle relazioni con tutte le classi di interlocutori.

Il Codice Etico è stato elaborato separatamente dal presente Modello ma ne costituisce parte integrante.

2.8. Presupposti del Modello

Sempre nel rispetto delle linee guida di Confindustria nel creare il proprio modello, Cyber-Bee srl è partita dalla propria struttura funzionale e da lì ha individuato le aree in grado potenzialmente di compiere reati e con quale grado di probabilità. In particolare, il Modello assicura:

- **efficacia ed efficienza**, ovvero un giusto rapporto tra risorse impiegate nel sistema dei controlli e risultati aggiunti;
- **informazione** ovvero report tempestivi per chi deve assumere decisioni;
- **corrispondenza** ovvero conformità delle azioni regole aziendali.

In particolare, il sistema di controllo interno si basa sui seguenti elementi:

- organigramma chiaro e preciso e relativo mansionario;
- sistema procedurale;
- sistemi informatici tali da permettere la separazione delle funzioni;
- sistema di controllo di gestione e reporting;
- poteri autorizzativi e di firma corrispondenti in maniera univoca al mansionario e assegnati incoerenza con le responsabilità;
- sistema organizzativo formalizzato e chiaro nell'attribuzione delle responsabilità;
- circolazione delle informazioni e formazione del personale.

Alla base del sistema di controllo interno di Cyber-Bee srl vi sono i seguenti principi:

- Ogni operazione, transazione, azione deve essere veritiera, verificabile, coerente e documentata.
- Nessuno deve poter gestire un intero processo in autonomia (c.d. segregazione dei compiti).
- Il sistema di controllo interno deve poter documentare l'effettuazione dei controlli, anche di supervisione.
- Tutto il personale, nell'ambito delle funzioni svolte, è responsabile della definizione e del corretto funzionamento del sistema di controllo attraverso i controlli di linea, costituiti dall'insieme delle attività di controllo che le singole unità operative svolgono sui loro processi.

2.9. Adozione e gestione del Modello nell'ambito di Cyber-Bee srl

Il modello è stato adottato da Cyber-Bee srl e sono seguite revisioni di aggiornamento approvate dall'Amministratore Unico.



2.10. Individuazione delle attività “a rischio”

La Società ha condotto un’attenta analisi dei propri strumenti di organizzazione, gestione e controllo, diretta a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto e, ove si sia reso necessario, ad adeguarli.

Nel rispetto del Decreto (art. 6, comma 2, lett. a) il Modello individua le attività aziendali, nel cui ambito possono essere potenzialmente commessi i reati da prevenire/evitare e per i quali le condotte illecite sono vietate e sanzionate.

È stata, dunque, condotta l’analisi delle attività aziendali di Cyber-Bee srl e delle relative strutture organizzative, allo specifico scopo di identificare le aree di attività aziendale a rischio in cui possono essere commessi i reati previsti dal Decreto, nonché i processi nel cui svolgimento potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato (cosiddetti processi “strumentali/funzionali”).

L’individuazione delle aree a rischio è dettagliatamente specificata nella “Parte Speciale – il MOGC”.

2.11. Principi di controllo interno generali

Sono:

- esplicita formalizzazione delle norme comportamentali;
- chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna direzione e alle diverse qualifiche e ruoli professionali;
- precisa descrizione delle attività di controllo e loro tracciabilità;
- adeguata segregazione di ruoli operativi e ruoli di controllo;
- Codice Etico;
- definizione dei ruoli temperando la pubblicità delle segnalazioni dei rischi e delle condotte, con la protezione del dichiarante.

In particolare, devono essere perseguiti i seguenti principi generali di controllo interno:

Norme comportamentali

Effettività di un Codice di Condotta/Etico che elenca in maniera descrittiva regole a carattere generale a salvaguardia delle attività svolte.

Definizioni di ruoli e responsabilità

- La normazione aziendale che individua ruoli e responsabilità di tutte le unità organizzative, perché, tra l’altro, descrive in maniera esaustiva le attività proprie di ciascuna struttura.
- Le norme sono rese disponibili e conosciute all’interno dell’organizzazione aziendale.

Procedure e norme interne

- Tutte le attività, in special modo quelle “sensibili” sono disciplinate, in modo coerente e congruo, attraverso la regolamentazione aziendale. Si è scelto il regolatorio più esaustivo per non lasciare aree prive di norme comportamentali, al fine di identificare anche i controlli e le responsabilità di chi opera in azienda, circolarizzando gli interventi di conoscenza dei singoli compiti, con protezione di anonimato e incolumità dei denunciati.
- Per ogni attività “sensibile” sono stati individuati e formalizzati i responsabili, coincidenti con quelli della struttura organizzativa competente per la gestione dell’attività stessa.



Segregazione dei compiti

- L'autonomia delle componenti organiche della struttura organizzativa aziendale consente la separazione tra chi, nell'ambito di ciascuna Funzione decide e chi materialmente la attua, la evidenzia documentalmente e la controlla.
- Tale separazione è lasciata che sia non solo funzionale ma anche soggettiva.

Poteri autorizzativi e di firma

- Al mansionario aziendale corrisponde un sistema di deleghe di poteri coerente con i compiti assegnati e tale da far sempre individuare il Funzionario responsabile. Eventuali limiti alle sue prerogative devono, chiaramente, essere rese note e pubbliche.
- Le procure sono coerenti con il sistema interno delle deleghe.
- Coerentemente con la normativa civilistica sono previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni.
- Il sistema di deleghe identifica, tra l'altro:
 - i requisiti e le competenze professionali che il delegato deve possedere 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;
 - le modalità operative di gestione degli impegni di spesa.

Vi è così rispondenza tra:

- l'autonomia decisionale e finanziaria del delegato;
- l'idoneità tecnico-professionale del delegato;
- la disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- Nell'ambito delle procedure o di altra regolamentazione interna sono formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità).
- La risultanza documentale inerente alle attività sensibili è formalizzata e irrigidita dagli obblighi redazionali della data di compilazione, della presa visione del documento e della firma riconoscibile del compilatore/supervisore; è stato predisposto un luogo idoneo alla conservazione delle documentazioni di verifica, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti.
- A posteriori e in qualsiasi momento deve poter essere documentato il processo di formazione degli atti e delle relative autorizzazioni, lo sviluppo delle operazioni, i materiali e le registrazioni degli atti, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate.
- È compito del responsabile dell'attività produrre e mantenere adeguati report di monitoraggio che evidenzino i controlli effettuati e delle eventuali anomalie riscontrate.
- Tutte le procedure di controllo sono gestite da procedure informatiche che garantiscano la corretta e veritiera imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile e ai soggetti che vi partecipano. Il sistema prevede l'impossibilità di modifica (non tracciata) delle registrazioni.



- I documenti sono archiviati e conservati, a cura della direzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza.
- L'accesso ai documenti già archiviati è sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a loro delegato, al Collegio Sindacale o ad organo equivalente o ad altri organi di controllo interno e all'Organismo di Vigilanza.



SEZIONE TERZA

3. ORGANISMO DI VIGILANZA

3.1 Funzioni e poteri dell'Organismo di Vigilanza

Funzioni dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sul funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

Tali compiti sono svolti dall'Organismo attraverso le seguenti attività:

- vigilanza sulla diffusione nel contesto aziendale della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilanza sulla validità ed adeguatezza del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto aziendale;
- verifica dell'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal Decreto; propone l'aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e/o adeguamenti dello stesso, in relazione alle mutate condizioni legislative e/o aziendali (cfr. par. 5 "Aggiornamento del Modello").

Nello svolgimento di dette attività, l'Organismo ha poteri per i seguenti adempimenti:

- collaborare con la direzione aziendale competente nella programmazione di un piano periodico di formazione volto a favorire la conoscenza delle prescrizioni del Modello di Cyber-Bee, differenziato secondo il ruolo e la responsabilità dei destinatari;
- istituire specifici canali informativi "dedicati" (indirizzo di posta elettronica dedicato), diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- garantire l'anonimato, la protezione, l'incolumità dei dichiaranti ogni segnalazione di rischio, potenziale condotta illecita, illecito perpetrato in danno di Cyber-Bee e contro i precetti della Legge;
- verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello.

Al fine di consentire all'Organismo la miglior conoscenza in ordine all'attuazione del Modello, alla sua efficacia e al suo effettivo funzionamento, nonché alle esigenze di aggiornamento dello stesso, è stato consentito che l'Organismo di Vigilanza operi in stretta collaborazione con le Direzioni aziendali, il Board, il Consiglio di Amministrazione.

Poteri dell'Organismo di Vigilanza

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- accedere liberamente, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D.lgs. 231/2001;
- disporre che i responsabili delle Direzioni aziendali, e in ogni caso tutti i Destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- dettare regole di protezione dei dichiaranti notizie di fatti inerenti agli illeciti che l'Organismo di Vigilanza denuncia di rilievo per le responsabilità di Cyber-Bee;



- ricorrere a consulenti esterni nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello.

3.2 Reporting dell'Organismo di Vigilanza

L'Organismo di Vigilanza provvede alla formalizzazione della sua attività istituendo anche un libro verbali (sul modello di quello del Collegio Sindacale) ove rende traccia del suo operato. Rimane comunque l'obbligo di informare tempestivamente l'Organo amministrativo e/o il Collegio Sindacale e/o l'Assemblea dei Soci se dovesse ravvisare accadimenti di irregolarità.

3.3 Flussi informativi nei confronti dell'Organismo di Vigilanza

Sono istituiti concreti ed effettivi obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza, secondo quanto previsto dai protocolli adottati e nelle singole Parti Speciali del Modello.

Per ciascuna "area a rischio reato" sono identificati uno o più "Responsabili Interni" che dovranno, tra l'altro, fornire all'Organismo di Vigilanza almeno con cadenza semestrale, i flussi informativi così come dallo stesso definiti. Anche nel caso in cui, nel periodo selezionato, non vi siano state segnalazioni significative da comunicare all'Organismo di Vigilanza, allo stesso dovrà essere inviata una segnalazione "negativa".

Sono stati inoltre istituiti precisi obblighi gravanti sugli organi sociali e sul personale di Cyber-Bee srl, in particolare:

- gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello;
- i Destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni delle prescrizioni del Modello o fattispecie di reato;
- vi è effettività di procedura delle protezioni dei dichiaranti fatti illeciti in danno di Cyber-Bee srl.

A tali fini è istituito un canale di comunicazione per la consultazione dell'Organismo di Vigilanza, consistente in un indirizzo di posta elettronica dedicato, e precisamente odv@cyber-bee.it finalizzato alla ricezione di segnalazioni. Tale modalità di trasmissione delle segnalazioni è volta a garantire la riservatezza dei segnalanti anche al fine di evitare atteggiamenti ritorsivi nei loro confronti.

L'Organismo di Vigilanza ha poteri di piena valutazione delle segnalazioni pervenutegli; può convocare, qualora lo ritenga opportuno, sia il segnalante per ottenere maggiori informazioni, assicurandogli la necessaria riservatezza, che il presunto autore della violazione; può procedere a tutti gli accertamenti e le indagini che siano necessarie per appurare la fondatezza della segnalazione.

Le segnalazioni devono essere in forma scritta e non anonima. È garantito l'anonimato.

Oltre alle segnalazioni sopra indicate, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, 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 assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- attività di controllo svolte dai responsabili di altre direzioni 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 (ivi compresi i provvedimenti verso i dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;



- segnalazione di infortuni gravi (omicidio colposo o lesioni colpose gravi o gravissime, in ogni caso qualsiasi infortunio con prognosi superiore ai 40 giorni) occorsi a dipendenti, addetti alla manutenzione, appaltatori e/o collaboratori presenti nei luoghi di lavoro della Società.

È stato previsto che tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite, per almeno cinque anni, dall'Organismo di Vigilanza, avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

Cyber-Bee srl nel corso del 2023 ha reso operativa la procedura sul whistleblowing, con cui sono state recepite le indicazioni contenute nel D.lgs. n. 24/2023 e valorizzati i principi di cui alle Linee Guida ANAC. Tale procedura, che è stata oggetto di aggiornamento in data 26 Febbraio 2025, è parte integrante del presente Modello.

In particolare, la nuova normativa introduce alcuni principi di massima richiamati all'interno del documento, tra cui si segnalano: (i) la tutela della riservatezza dell'identità del segnalante e delle persone menzionate nella segnalazione; (ii) la protezione da ritorsioni; (iii) l'istituzione di canali interni ed esterni per la segnalazione e (iv) il riscontro al segnalante in ordine alla ricezione e all'esito finale della segnalazione.

La Società, al fine di rafforzare i presidi di controllo esistenti in materia di whistleblowing, ha ritenuto opportuno introdurre un sistema informatizzato per la gestione delle segnalazioni che consente di garantire la tutela dell'identità del segnalante, permettendo altresì la trasmissione di segnalazioni in forma anonima, nel rispetto del principio di segregazione.

La società Cyber-Bee srl ha altresì provveduto, per garantire una effettiva conoscenza del D.lgs. n. 24/2023 e un esercizio consapevole del diritto alla segnalazione, ad effettuare un'adeguata formazione del personale.

Cyber-Bee srl ha individuato nell'OdV il destinatario delle segnalazioni in materia di whistleblowing, effettuate dai soggetti interni, sia apicali che sottoposti.

Per effettuare le segnalazioni contemplate dal menzionato d.lgs. 24/2023, Cyber-Bee srl ha messo a disposizione di tutti i soggetti legittimati l'utilizzo di una specifica piattaforma informatica denominata "*Whistleblowing*" raggiungibile digitando il link (<https://whistleblowing.cyber-bee.it/>), piattaforma conforme ai dettami del d.lgs. 24/2023, nonché alle indicazioni ed alle caratteristiche contenute nelle Linee Guida ANAC.

Questo meccanismo consente ai dipendenti e ad altri soggetti di segnalare attività illegali, comportamenti scorretti o violazioni delle normative in modo riservato e senza timore di ritorsioni. La procedura di whistleblowing promuove la trasparenza, l'integrità e la responsabilità aziendale, contribuendo a creare un ambiente più etico e sostenibile.

Per l'iter di segnalazione si rimanda alla relativa procedura. Al seguente link [https://cyber-bee.it/Procedura Whistleblowing Cyber-Bee 2025.pdf](https://cyber-bee.it/Procedura_Whistleblowing_Cyber-Bee_2025.pdf) nella sezione RESPONSIBILITY è possibile reperire tutte le informazioni inerenti il contenuto delle segnalazioni e le modalità di presentazione, ovvero la procedura *Whistleblowing*.

In merito al contenuto delle segnalazioni si specifica che possono essere segnalate tutte quelle situazioni in grado di arrecare danno o pregiudizio alla Società come:

- condotte illecite rilevanti ai sensi del D.Lgs.231/01 riconducibili a qualunque reato o tentativo di reato incluso nel novero dei reati presupposto del D.Lgs.231/01 quali ad esempio: corruzione di pubblici ufficiali o incaricati di pubblico servizio, malversazione a danno dello Stato, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, corruzione tra privati, associazione a delinquere, false comunicazioni sociali, riciclaggio, ricettazione, autoriciclaggio, agiotaggio, frode in commercio, reati in materia di salute e sicurezza sul lavoro, reati ambientali, reati contro la personalità individuale, reati di criminalità informatica;
- violazioni del Modello 231 o del Codice di Condotta adottati dalla Società, poste in essere dai Soggetti Segnalati e di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali condotte, ancorché non integranti le fattispecie dei reati rilevanti ai sensi del D.Lgs. 231/01, possono ad esempio riguardare violazioni delle Parti Speciali del Modello 231 o degli altri protocolli di prevenzione (ovvero i principi di comportamento e le procedure di controllo che regolamentano lo



svolgimento delle attività sensibili) ivi inclusi i provvedimenti interni, gli atti e le procedure operative adottate dalla Società che costituiscono attuazione dei contenuti del Modello 231.



SEZIONE QUARTA

4. SISTEMA DISCIPLINARE

Aspetto essenziale per l'effettività del Modello è costituito dalla disciplina e dal sistema sanzionatorio delle condotte poste in essere in violazione delle regole sulla prevenzione dei reati di cui al Decreto, e, in generale, delle procedure interne previste dal Modello stesso.

L'applicazione delle sanzioni disciplinari è indipendente dalle risultanze processuali penali, in quanto le regole di condotta imposte dal Modello sono state adottate dall'azienda in piena autonomia senza avere la pretesa di ricalcare eventuali norme giuridiche corrispondenti.

A tal proposito, Il R1 Group ha adottato un sistema disciplinare elaborato separatamente, "Parte Generale – Il Sistema Disciplinare, che è parte integrante del presente Modello. Cyber-Bee srl ha esemplificato a tutti i propri lavoratori dipendenti con rapporto di lavoro di natura subordinata che la violazione del Sistema obbligatorio del Codice Etico è sanzionata disciplinarmente (art.7 Statuto dei Lavoratori) per averne esplicitato la priorità tra i doveri dei Lavoratori (cfr. Codice Disciplinare Aziendale effettivo e pubblicato in bacheca aziendale).

5. AGGIORNAMENTO DEL MODELLO

Il presente Modello è da ritenersi "dinamico" e non statico e viene aggiornato parallelamente al mutare della realtà aziendale e/o legislativa e/o comunque di riferimento. È funzionalizzato alle esigenze concrete dell'Azienda Cyber-Bee srl e ottiene ritorno ispettivo con la continuativa formazione evolutiva che impartisce ai responsabili di area organizzativa.

6. INFORMAZIONE E DIFFUSIONE DEL MODELLO TRA I PORTATORI D'INTERESSE

Con l'adozione di questo Modello Organizzativo, Cyber-Bee srl ha deciso anche di strumentalizzare la pubblicazione degli impegni e delle regole prescelte perché l'efficacia della propria scelta virtuosa sia garantita tramite gli impegni e le potestà attribuite ai destinatari del Codice e del Modello stesso.

Si riportano di seguito le attività individuate per una corretta ed esaustiva comunicazione e divulgazione del Modello a tutti gli Stakeholder.

Le Risorse Umane di Cyber-Bee srl, presenti e future, sono costantemente informate e aggiornate oltre che per il tramite dei canali tradizionali (ordini di servizio, circolari, etc.) anche mediante meeting, riunioni periodiche e corsi di formazione. In particolare, Cyber-Bee srl garantisce:

- la comunicazione a tutti i dipendenti dell'avvenuta adozione del Modello ex D.lgs. 231/2001 e dei successivi aggiornamenti approvati, e la diffusione del Modello (in formato elettronico e/o cartaceo e rilascio di una dichiarazione di avvenuta ricezione e accettazione);
- la comunicazione a tutti i dipendenti delle parti operative del modello di loro interesse;
- la consegna ai nuovi dipendenti di un'apposita informativa sul Modello adottato (es. informativa specifica da consegnare insieme ad altra documentazione al momento dell'assunzione);
- l'attività di formazione periodica finalizzata a diffondere la conoscenza della normativa di cui al Decreto, differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società.

Per tutti gli altri Destinatari, Cyber-Bee srl ha sempre l'impegno di rendere loro specifica:



- comunicazione dell'adozione del Modello vigente perché tutti i soggetti/partner che intrattengano, direttamente o indirettamente, con Cyber-Bee srl rapporti contrattualmente regolati siano resi edotti degli impegni e degli obblighi che il Modello impone anche a loro;
- segnalazione dell'obbligo che gli è richiesto di aderire al Codice Etico mediante espressione inequivoca di conoscenza delle disposizioni del D.lgs. 231/2001 e delle prescrizioni del Modello e di impegno al rispetto dello stesso. Le dichiarazioni dei Destinatari sono prioritariamente raccolte in qualunque contratto di fornitura, servizio e consulenza, trascritte nel corpo del testo negoziale e/o in specifico allegato.

