NEVERHACK

FRANCIA | BELGIO | CANADA |
ESTONIA | ITALIA | SPAGNA |
MESSICO | SINGAPORE | UAE | USA |

/NEVERHACK ITALY S.p.A.

Modello di Organizzazione, Gestione e Controllo - Parte Generale

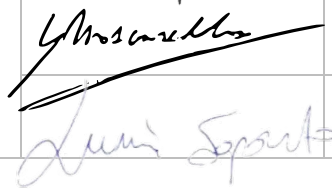
MOGC-GEN

Document information

Revision Log

Date	Version	Author	Change
06/10/2025	1.0	Consulente esterno	Redazione e revisione della politica

Approval

23/12/2025	Validated by		Head of Risk & Compliance Davide Fusco
29/12/2025	Approved by		Amministratore Delegato Guido Moscarella
			Presidente OdV Livia Saporito

Change Log

Version	Change
1.0	First release

Sommario

1 Introduzione: il Gruppo Neverhack e l'idea di MOGC di Neverhack Italy

Il Gruppo Neverhack e la controllata Neverhack Italy S.p.A., nel misurarsi con la disciplina della Responsabilità Amministrativa degli Enti da Reato e nella conseguente adozione di un Modello di Organizzazione, Gestione e Controllo (MOGC), hanno intrapreso una profonda rivalutazione del sistema dei processi e delle procedure aziendali. Tale percorso ha consentito di valorizzare appieno il capitale umano, culturale e tecnico che caratterizza il Gruppo e le persone che ne fanno parte.

Grazie a un'attività congiunta e coordinata della "Gente di Neverhack", coinvolta direttamente in ogni fase, è stato sviluppato un sistema di controllo **tailor made**, dinamico e in costante evoluzione. Le procedure, poste a sostegno del Modello, ne costituiscono la struttura portante e sono integrate da controlli mirati all'emersione delle anomalie di processo, nonché da meccanismi automatici di segnalazione alle funzioni di controllo. Questi strumenti, attivandosi in tempo reale e coinvolgendo più soggetti, rendono il Modello, le procedure e i sistemi di controllo e segnalazione costantemente interconnessi.

Il sistema, pur comportando un significativo impegno per l'Ente – sia per l'ampiezza delle procedure adottate, sia per il coinvolgimento delle diverse funzioni nelle varie fasi di processo – riduce drasticamente il rischio di commissione di reati e consente di intervenire nell'immediatezza ove emergano criticità, implementando le *best practice* aziendali.

Il presente Modello di Organizzazione, Gestione e Controllo (di seguito anche "Modello" o "MOG") è adottato da Neverhack Italy S.p.A. ai sensi e per gli effetti del Decreto Legislativo 8 giugno 2001, n. 231, con l'obiettivo di prevenire la commissione dei reati presupposto previsti dal Decreto, nonché di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Il Modello è stato elaborato sulla base di una specifica attività di risk assessment, condotta mediante l'analisi dei processi aziendali rilevanti, l'individuazione delle aree a rischio di commissione dei reati presupposto, la valutazione del livello di rischio (in termini di probabilità e impatto) e la definizione di idonei presìdi di controllo, preventivi e di monitoraggio.

Il Modello si fonda sui principi di tracciabilità delle attività, segregazione delle funzioni, attribuzione formale di responsabilità, documentabilità dei controlli e verificabilità delle decisioni, ed è strutturato in modo da consentire un costante aggiornamento in relazione all'evoluzione normativa, organizzativa e operativa della Società.

La scelta è stata compiuta anche a seguito di un esame di merito relativo al mercato in cui opera la società, caratterizzato da rapidi salti di innovazione che rendono obsoleto ciò che fino a poco prima appariva futuristico e che finiscono per travolgere il sistema regolatorio posto alle sue soglie.

La creazione di tale sistema non sarebbe stata possibile senza la piena consapevolezza dell'obiettivo da parte di tutte le risorse coinvolte, dalle figure apicali alle singole funzioni operative.

2 Premessa

2.1 Il Decreto Legislativo n. 231/2001 e successive modifiche e integrazioni

In data 8 giugno 2001, con il Decreto Legislativo n. 231 (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio 2001, il Legislatore ha recepito nel nostro ordinamento quanto stabilito nelle convenzioni internazionali in materia di responsabilità delle persone giuridiche.

Il Decreto, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", ha introdotto un regime di responsabilità amministrativa a carico degli enti, che si aggiunge alla responsabilità penale della persona fisica che ha materialmente commesso il reato.

L'indicazione, nel Decreto, di "responsabilità amministrativa" è formalmente esatta, anche se, sostanzialmente, la natura delle gravi sanzioni previste e la valutazione da parte dello stesso Giudice penale che tratta il processo a carico dell'imputato indicano trattarsi di una forma di responsabilità strettamente legata alla responsabilità penale della persona fisica in ragione tanto della rappresentanza organica del soggetto quanto dell'appartenenza del fatto costitutivo di reato nella sua dimensione oggettiva all'ente. La responsabilità dell'ente ai sensi del D.Lgs. n. 231/2001 costituisce così un *tertium genus* rispetto a responsabilità penale e responsabilità amministrativa e converge con la responsabilità penale della persona fisica. La responsabilità dell'ente è strettamente collegata alla commissione di un reato, tanto che il fatto di reato di cui risponde la persona fisica è anche fatto dell'ente che risponde del peculiare illecito di cui al D.Lgs. n. 231/2001. Trattandosi di fatto appartenente a entrambi, persona fisica e persona giuridica, lo schema è quello della responsabilità concorsuale che si articola diversamente in relazione alla diversa natura dei soggetti chiamati a rispondere del medesimo fatto.

La responsabilità dell'Ente sorge soltanto in occasione della realizzazione di determinati tipi di reato da parte di soggetti legati a vario titolo all'ente medesimo e solo nell'ipotesi che la condotta illecita sia stata realizzata nell'"interesse o a vantaggio" di esso: non soltanto, quindi, allorché il comportamento illecito abbia determinato un vantaggio, patrimoniale o meno per l'ente, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell'interesse dell'ente.

La Relazione governativa che accompagna il Decreto chiarisce che il richiamo all'interesse dell'ente caratterizza «in senso marcatamente soggettivo la condotta (…) della persona fisica» e si "accontenta" di una verifica *ex ante*. Viceversa, il vantaggio, che può essere tratto dalla società anche quando l'autore del fatto non abbia agito nel suo interesse, richiede sempre una verifica *ex post*.

Gli enti possono essere ritenuti responsabili per alcuni reati commessi o tentati, nel loro interesse o vantaggio da:

a) persona fisica che rivesta funzioni di rappresentanza, amministrazione, direzione, anche di un'unità organizzativa dell'ente dotata di autonomia finanziaria e funzionale;
b) persone che esercitino, anche in via di fatto, la gestione o il controllo dell'ente stesso;
c) soggetti sottoposti alla direzione o vigilanza di chi gestisce o controlla l'ente.

La responsabilità degli enti è indipendente da quella della persona fisica che ha realizzato il fatto nell'interesse o a vantaggio dell'ente stesso. Essa, infatti, sussiste anche quando l'autore del reato non sia stato identificato o non sia imputabile e quando il reato si estingua per una causa diversa dall'amnistia.

Il D.Lgs. n. 231/2001 **ha diversificato il sistema di responsabilità dell'ente** a seconda che il reato sia stato commesso da un soggetto in posizione apicale o da un soggetto sottoposto alla direzione o alla vigilanza di un soggetto in posizione apicale.

È opportuno precisare che **l'ente non risponde**, per espressa previsione legislativa (art. 5, comma 2, del D.Lgs. n. 231/2001), **se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi**.

Nelle ipotesi in cui il reato sia stato commesso da **soggetti in posizione apicale** (sono considerati tali i soggetti specificati nelle lettere a) e b) del presente paragrafo), l'imputabilità all'ente è presunta.

L'art. 6, comma 1, del Decreto prevede che, qualora il reato sia commesso dagli apicali, l'ente non risponde se prova che:

a. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
b. il compito di vigilare sul funzionamento e l'osservanza dei modelli 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 reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
d. non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lett. b).

Qualora il reato sia stato realizzato da un **soggetto in posizione subordinata** (ovvero da uno dei soggetti descritti nella lettera c) del presente paragrafo), l'ente sarà responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza (art. 7, comma 1 D.Lgs. n. 231/2001). In ogni caso, si presume *iuris et de iure* l'osservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2 D.Lgs. n. 231/2001).

I successivi commi 3 e 4 dell'art. 7 D.Lgs. n. 231/2001 introducono due principi che, sebbene siano collocati nell'ambito della norma sopra rammentata, appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'Ente per entrambe le ipotesi di reato di cui all'art. 5 lettere a) e b). Segnatamente è previsto che:

- il Modello deve prevedere misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività condotta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione; assume rilevanza altresì l'esistenza di un idoneo sistema disciplinare (condizione già prevista dalla lettera e) sub art. 6 comma 2).

Sotto un profilo formale, l'adozione e l'efficace attuazione di un Modello non costituisce un obbligo, ma unicamente un onere per gli Enti i quali, invero, potranno anche decidere di non conformarsi al disposto del Decreto senza incorrere per ciò solo in alcuna sanzione.

Tuttavia, l'adozione e l'efficace attuazione di un Modello idoneo è per gli Enti un presupposto irrinunciabile per poter beneficiare dell'esimente prevista dal Legislatore.

È importante, inoltre, considerare che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette all'Ente di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali carenze che, al momento della sua creazione, non era possibile individuare.

Ai sensi dell'art. 6, comma secondo del Decreto, il modello organizzativo deve rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi i reati cui si applica la normativa 231;
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 a impedire la commissione dei reati;
d) prevedere obblighi di informazione nei confronti dell'Organo di Vigilanza (OdV), deputato a vigilare sul funzionamento e l'osservanza del Modello;
e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

La responsabilità dell'ente non scaturisce dalla commissione da parte dei soggetti appena individuati di qualsivoglia fattispecie criminosa, ma è circoscritta alle ipotesi di reato previste originariamente dal D.Lgs. n. 231/2001 e dalle successive modifiche legislative. Da rilevare, tuttavia, che il catalogo dei reati c.d. "presupposto" è in continua espansione.

2.2 Le sanzioni previste dal D.Lgs. n. 231/2001

L'**articolo 9, comma 1, del Decreto** individua le sanzioni che possono essere applicate all'ente per gli illeciti amministrativi dipendenti da reato, ovvero:

1) la sanzione pecuniaria;
2) le sanzioni interdittive;
3) la confisca;
4) la pubblicazione della sentenza.

Da un punto di vista generale, è opportuno precisare che l'accertamento della responsabilità dell'Ente, nonché la determinazione dell'*an* e del *quantum* della sanzione, sono attribuiti al Giudice penale competente per il procedimento relativo ai reati dai quali dipende la responsabilità amministrativa (art. 36 D.Lgs. n. 231/2001).

L'Ente è ritenuto responsabile dei reati individuati dagli artt. 24 ss. anche se questi siano realizzati nelle forme del tentativo. In tali casi, però, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà (art. 26, comma 1 D.Lgs. n. 231/2001).

L'Ente non risponde quando volontariamente impedisca il compimento dell'azione o la realizzazione dell'evento (art. 26, comma 2 D.Lgs. n. 231/2001).

Le **"sanzioni pecuniarie"** trovano regolamentazione negli artt. 10, 11 e 12 del Decreto e si applicano in tutti i casi in cui sia riconosciuta la responsabilità dell'Ente. Le sanzioni pecuniarie vengono applicate per quote, in numero non inferiore a 100 e non superiore a 1000, mentre l'importo di ciascuna quota va da un minimo di 258,23 € a un massimo di 1.549,37 €. Il Giudice determina il numero delle quote sulla base degli indici individuati dal primo comma dell'art. 11, mentre l'importo delle quote è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente coinvolto.

Le **"sanzioni interdittive"**, individuate dal comma II dell'art. 9 del Decreto e irrogabili nelle sole ipotesi tassativamente previste e solo per alcuni reati, sono:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;
- il divieto di pubblicizzare beni o servizi.

Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinate dal Giudice penale che conosce del processo per i reati commessi dalle persone fisiche, tenendo conto dei fattori meglio specificati dall'art. 14 del Decreto. In ogni caso, le sanzioni interdittive hanno una durata minima di 3 mesi e massima di 2 anni (art. 13, comma 3 D.Lgs. n. 231/2001).

L'art. 1 della legge 9 gennaio 2019 n. 3 ha modificato il comma 2 dell'art. 13, innalzando la durata delle sanzioni interdittive – da 4 a 7 anni se il reato è stato commesso da uno dei soggetti di cui all'art. 5 comma 1 lett. a) e da 2 a 4 anni se il reato è stato commesso da uno dei soggetti di cui all'art. 5 comma 1 lett. b) – in relazione ai delitti di cui all'art. 25 commi 2 e 3 D.Lgs. n. 231/2001, salvo che ricorrano le condizioni di cui al comma 5 bis.

Ai sensi dell'art. 13 del D.Lgs. n. 231/2001, le sanzioni interdittive possono essere applicate all'Ente all'esito del giudizio, accertata la colpevolezza dello stesso, quando ricorre almeno una delle seguenti condizioni:

- l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative (art. 13, comma 1 lett. *a*, D.Lgs. n. 231/2001);
- in caso di reiterazione degli illeciti (art. 13, comma 1 lett. *b*, D.Lgs. n. 231/2001).

In virtù dell'art. 45 D.Lgs. n. 231/2001, le sanzioni interdittive possono essere applicate in via cautelare qualora sussistano gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi siano fondati e specifici elementi che fanno ritenere concreto il pericolo di commissione di reati della stessa indole di quello per cui si procede.

La **confisca** del prezzo o del profitto del reato è una sanzione obbligatoria che consegue all'eventuale sentenza di condanna (art. 19 Decreto).

La **pubblicazione della sentenza** è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva (art. 18 Decreto).

2.3 L'adozione e l'attuazione di un Modello di Organizzazione, Gestione e Controllo quale esimente della responsabilità amministrativa da reato

Il Legislatore riconosce, agli artt. 6 e 7 del Decreto, **forme specifiche di esonero della responsabilità amministrativa dell'Ente**.

In particolare, l'art. 6, comma 1°, del Decreto prevede che, qualora il reato sia commesso dagli apicali, l'ente non risponde se prova che:

a. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b. il compito di vigilare sul funzionamento e l'osservanza dei modelli 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 reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d. non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lett. b).

Il contenuto dei Modelli è individuato dallo stesso art. 6, il quale, al co. 2°, prevede che essi "devono rispondere alle seguenti esigenze:

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

Qualora, invece, il reato sia commesso da soggetti in posizione subalterna, l'ente risponde se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza (art. 7, comma 1 D.Lgs. n. 231/2001). In ogni caso, si presume *iuris et de iure* l'osservanza degli obblighi di direzione o vigilanza se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2 D.Lgs. n. 231/2001).

I successivi commi 3 e 4 dell'art. 7 D.Lgs. n. 231/2001 introducono due principi che, sebbene siano collocati nell'ambito della norma sopra rammentata, appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'Ente per entrambe le ipotesi di reato di cui all'art. 5 lettere a) e b).

Segnatamente è previsto che:

- il Modello deve prevedere misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione; assume rilevanza altresì l'esistenza di un idoneo sistema disciplinare (condizione già prevista dalla lettera e) sub art. 6 comma 2).

Sotto un profilo formale, l'adozione e l'efficace attuazione di un Modello non costituisce un obbligo, ma unicamente un onere per gli Enti, i quali, invero, potranno anche decidere di non conformarsi al disposto del Decreto, i quali possono anche scegliere di non conformarsi alle disposizioni del Decreto, senza per questo incorrere in alcuna sanzione.

Tuttavia, l'adozione e l'efficace attuazione di un Modello idoneo è per gli Enti un presupposto irrinunciabile per poter beneficiare dell'esimente prevista dal Legislatore.

È importante, inoltre, considerare che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette all'Ente di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali mancanze che, al momento della sua creazione, non era possibile individuare.

2.4 Le Linee Guida di Confindustria

Nella costruzione del presente Modello, Neverhack Italy, oltre all'osservanza delle prescrizioni indicate dal Decreto, ha seguito i principi espressi nelle Linee Guida predisposte da Confindustria nell'ultimo aggiornamento.

Gli aspetti salienti di tali linee (nel seguito denominate "Linee Guida") possono essere così sintetizzati:

a) identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quale area o settore di attività e secondo quali modalità potrebbero verificarsi eventi pregiudizievoli agli obiettivi perseguiti dal D.Lgs. n. 231/01;

b) progettazione del sistema di controllo, ovvero di protocolli finalizzati a programmare sia la formazione che l'attuazione delle decisioni dell'ente, in relazione ai reati da prevenire.

Proprio in funzione della realizzazione di tali obiettivi, è stato previsto dalle Linee Guida un sistema di controllo, le cui componenti di maggior rilievo sono:

I. Codice Etico;

II. sistema organizzativo chiaro e formalizzato, con attribuzione di responsabilità, linee di dipendenza gerarchica, descrizione dei compiti e specifica previsione dei principi di controllo adottati;

III. procedure manuali e informatiche tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo;

IV. poteri autorizzativi e di firma, con puntuale indicazione dei limiti di approvazione delle spese;

V. sistema di controllo di gestione in grado di segnalare tempestivamente situazioni di particolare criticità;

VI. comunicazione al personale e programma di formazione.

c) individuazione di un Organismo di controllo (l'OdV) della Società con il compito di vigilare sull'efficacia, adeguatezza e applicazione del Modello (si veda, infra, par. 3.7.);

d) l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;

e) disciplina delle modalità di effettuazione delle segnalazioni cd. "whistleblowing".

3 Il Modello di Organizzazione, Gestione e Controllo di Neverhack Italy S.p.A.

3.1 L'attività di Neverhack Italy S.p.A. in breve

Il Gruppo Neverhack rappresenta una realtà consolidata nel panorama IT e della cybersecurity a livello globale, con una presenza in 10 Paesi, 1.200 collaboratori in tutto il mondo e una storia che affonda le proprie radici nei pionieri della consulenza in materia di sicurezza informatica in Francia, a partire dalla fondazione di Silicom nel 1983.

Nel 2019 nasce Seela, piattaforma online dedicata alla formazione dei team in ambito cybersecurity. Nel 2021 la storia prosegue con la fusione tra Silicom e Seela, da cui prende vita PrOph3cy. Opencyber, leader negli audit tecnici e nei penetration test, entra a far parte del gruppo insieme a Harmonie Technologie, realtà di riferimento nella consulenza strategica in cybersecurity.

Nel tempo Seela (PrOph3cy) evolve in un ecosistema dinamico, presentando tre prodotti innovativi: Cyber Unity per la sensibilizzazione, Cyber Training per la formazione e BattleHack per lo sviluppo di competenze avanzate.

Nel maggio 2023 il Gruppo Neverhack, recentemente rinominato, consolida la propria strategia e rafforza l'impegno verso i clienti ottenendo un investimento di 100 milioni di euro a sostegno delle iniziative di crescita esterna. Expert Line si unisce all'avventura Neverhack per potenziare il Security Operations Center (SOC), con l'obiettivo di prevenire, proteggere, rilevare e risolvere gli incidenti di sicurezza attraverso un monitoraggio continuo 24/7. Cybers, rinomata azienda di cybersecurity con sede in Estonia, entra nel gruppo, rafforzandone le competenze SOC ed espandendo le attività nel Nord Europa.

Nel 2024 Innovery, multinazionale leader nei servizi ICT e specializzata in cybersecurity, amplia le attività commerciali di Neverhack nell'Europa meridionale, in Messico e negli Stati Uniti, operando con il nome di Neverhack Italy.

Le principali attività del gruppo, rivolte prevalentemente a soggetti istituzionali, multinazionali e grandi gruppi industriali, possono essere sinteticamente ricondotte alla gestione di casi d'uso quali:

- **Δ** Team Awarness
- **Δ** Regolamentazione Informatica
- **Δ** Esposizioni Terze Parti
- **Δ** Rafforzamento Della Sicurezza
- **Δ** Crisi Informatiche
- **Δ** Contesto e Confronto
- **Δ** Livello di Privilegio
- **Δ** Protezione Dati Threat
- **Δ** Intelligence Problemi Di Sicurezza
- **Δ** Valutazione del Rischio Informatico
- **Δ** Preparazione e Disastri Informatici

La varietà delle attività del gruppo, la composizione eterogenea — seppur concentrata nei settori IT e cybersecurity —, la sua estensione geografica e la natura critica dei casi d'uso trattati, spesso con rilevanti implicazioni sistemiche ed economiche, hanno reso necessaria, nella redazione del MOGC di Neverhack Italy, un'analisi del rischio non solo conforme alle linee guida di Confindustria e al Cybersecurity Act (Regolamento UE 2019/881 del 17 aprile 2019), ma anche basata su un confronto diretto con ogni divisione operativa e funzione aziendale, per identificarne i rischi 231 diretti e indiretti.

L'oggetto sociale principale della Società consiste nella fornitura di servizi di cybersecurity (soluzioni per la sicurezza dei dati e delle reti) e, più in generale, nel supporto alla promozione, realizzazione e gestione di sistemi ICT per professionisti, aziende ed enti pubblici e privati (trattamento elettronico dei dati; realizzazione o integrazione di sistemi informativi, sistemi operativi, database, hardware di rete, file system e soluzioni di sicurezza).

La Società opera inoltre in Messico, Spagna e Stati Uniti attraverso società controllate o partecipate.

Neverhack Italy S.p.A. è certificata secondo le norme internazionali UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, UNI EN ISO 45001:2018 e UNI EN ISO 27001:2022.

La Società riconosce inoltre l'importanza della valutazione delle performance ambientali, sociali e di governance (ESG) ed è impegnata in una gestione proattiva del capitale umano e nella tutela dell'ambiente, riducendo l'impatto delle proprie attività anche attraverso la diminuzione dei consumi. A tal proposito, Neverhack Italy redige volontariamente un proprio bilancio di sostenibilità e aderisce al rating EcoVadis.

3.2 La Governance di Neverhack Italy S.p.A.

Neverhack ha optato per il sistema di amministrazione e controllo tradizionalmente previsto nell'ordinamento italiano: da un lato, l'amministrazione è affidata al Consiglio di Amministrazione; dall'altro, il Collegio Sindacale svolge le funzioni di controllo. Il controllo contabile, invece, è affidato ad una società di revisione.

Il Consiglio di Amministrazione (CdA) è investito dei più ampi poteri per la gestione della Società, senza eccezioni, ed è autorizzato a compiere tutti gli atti ritenuti opportuni per l'attuazione e il raggiungimento degli scopi sociali, fatta eccezione per quelli che la legge riserva in via esclusiva all'Assemblea dei soci. Tra le sue prerogative rientrano, tra l'altro, la definizione degli indirizzi strategici della Società e la verifica dell'adeguatezza ed efficienza dell'assetto organizzativo e amministrativo.

Il Consiglio di Amministrazione è composto da:

- Presidente del Consiglio di Amministrazione, che ha la rappresentanza della società.
- Amministratore Delegato a cui sono stati conferiti, in via disgiunta, i poteri di ordinaria amministrazione, fra cui, a titolo esemplificativo e non esaustivo: legale rappresentanza della Società; stipula dei contratti di lavoro e gestione del personale; stipula di contratti attivi e passivi, anche con riferimento allo sviluppo dell'attività commerciale della Società; riscossione di somme a qualunque titolo e per qualsiasi ragione dovute alla Società; effettuazione di operazioni bancarie di qualsivoglia natura (es. aprire conti correnti, operare su conti correnti, chiedere e usufruire di affidamenti bancari, richiedere il rilascio di fideiussioni bancarie); stipula di contratti di assicurazione; rappresentanza della Società nei rapporti con le pubbliche amministrazioni, ecc.
    - Tali poteri comprendono anche le attività relative alla protezione dell'ambiente e alla gestione degli obblighi previsti dal GDPR.
    - L'Amministratore Delegato è inoltre rappresentante legale della Società in materia fiscale, con facoltà di sottoscrivere le relative dichiarazioni.
- Consigliere Delegato a cui sono stati conferiti, qualsiasi tipo di accordo per prestazioni di servizio e di carattere strategico finalizzati allo sviluppo commerciale della società, determinare le politiche di prezzo promozione distribuzione e acquisto di tutti i prodotti e servizi aziendali, gestire ogni aspetto della rete di vendita e senza limiti di spesa acquistare vendere e compiere tutte le attività precontrattuali e contrattuali nei confronti dei clienti, concorrere alle gare indette dalle amministrazioni statali, enti pubblici e privati.
- Consigliere Delegato individuato come Datore di Lavoro a titolo originario ai sensi dell'art. 2 del D.Lgs. n. 81/2008, cui sono attribuiti i necessari poteri decisionali e di spesa da esercitarsi in piena autonomia e senza limitazione alcuna per la tutela della salute e sicurezza dei lavoratori.
- Consigliere Delegato cui sono stati conferiti i poteri necessari per tutte le operazioni bancarie, ivi inclusa l'ordinaria gestione dei rapporti con gli istituti di credito.

La struttura organizzativa di Neverhack è formalizzata in un organigramma aziendale e nel documento "Ruoli Aziendali" che con chiarezza individua ruoli e responsabilità, le linee di dipendenza gerarchica e i legami funzionali tra le diverse posizioni di cui si compone la struttura stessa.

L'Organigramma aziendale, che rappresenta graficamente l'assetto organizzativo della Società, è un documento di emanazione del Consiglio di Amministrazione.

3.3 L'adeguamento di Neverhack Italy alle previsioni del Decreto Legislativo 231/2001

Neverhack Italy S.p.A., compreso e condiviso lo spirito della normativa di riferimento, ha ritenuto necessario implementare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della posizione e dell'immagine della Società e delle aspettative degli stakeholder. In tale prospettiva, ha considerato conforme alle proprie politiche aziendali procedere all'adozione del Modello di organizzazione e gestione previsto dal Decreto Legislativo n. 231/2001.

La decisione è stata assunta con l'obiettivo di rafforzare la struttura organizzativa e prevenire eventuali carenze che potrebbero agevolare la commissione di illeciti. Si è ritenuto, infatti, che l'adozione di un Modello organizzativo potesse costituire un efficace strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto, o comunque nell'interesse, di Neverhack Italy S.p.A., affinché adottino comportamenti corretti e coerenti nello svolgimento delle proprie attività, prevenendo così il rischio di commissione dei reati contemplati dal Decreto.

Con tale scelta, la Società ha inteso conformarsi pienamente al D.Lgs. n. 231/2001, il quale, pur non imponendo obbligatoriamente l'adozione del Modello, ne suggerisce espressamente l'implementazione ai sensi dell'art. 6.

3.4 I lavori preparatori alla redazione del modello organizzativo. La metodologia seguita per l'individuazione delle c.d. "aree a rischio"

Neverhack Italy S.p.A. ha proceduto all'elaborazione del Modello Organizzativo previa analisi dell'intera struttura aziendale e del sistema di controlli interni, per verificarne l'adeguatezza rispetto agli obiettivi di prevenzione dei reati rilevanti.

L'attività di *risk mapping* e *risk assessment* è stata condotta attraverso l'esame della documentazione aziendale (step 1) e mediante lo svolgimento di diverse sessioni di interviste (step 2).

All'esito di tale attività è stata effettuata una completa disamina della governance aziendale ed è stato predisposto un elenco dettagliato delle "aree a rischio reato", ossia quei settori della Società e/o processi aziendali nei quali, sulla base dei risultati della mappatura, è stato ritenuto astrattamente sussistente il rischio di commissione dei reati che possono fondare la responsabilità dell'Ente.

In particolare, si è proceduto a distinguere, da un lato, le aree direttamente esposte e, dall'altro, le cosiddette "aree strumentali", vale a dire quei settori nei quali possono realizzarsi condizioni di fatto idonee a rendere possibile la commissione di reati nelle aree direttamente esposte (ad esempio: selezione e assunzione del personale, sistemi di incentivazione, consulenze e prestazioni professionali, acquisizione di beni e servizi, sponsorizzazioni e spese di rappresentanza).

Per ciascuna area a rischio sono state individuate le *attività sensibili*, ossia quelle attività il cui svolgimento può comportare il rischio di commissione dei reati, nonché le funzioni aziendali coinvolte.

Per ogni attività sensibile sono state inoltre identificate, in via astratta, le possibili modalità di commissione dei reati considerati, tenendo conto delle diverse tipologie di illecito e delle modalità con cui tali reati potrebbero essere realizzati.

Sono state quindi individuate, per esclusione, le aree aziendali non interessate dal rischio reato.

La selezione sopra descritta è stata effettuata con la collaborazione attiva del management e dei dipendenti, ai quali, durante le interviste, è stato richiesto di verificare le procedure interne esistenti nelle aree individuate e di segnalare eventuali punti di miglioramento, formulando specifici suggerimenti.

Al termine dell'intero processo sono stati individuati gli interventi necessari per l'adeguamento e l'implementazione dei principi di controllo (*gap analysis*).

Le verifiche svolte hanno riguardato, in particolare, le seguenti componenti del sistema di controllo preventivo:

- **Sistema organizzativo** – La verifica dell'adeguatezza del sistema è stata effettuata sulla base della formalizzazione delle strutture, della chiara definizione delle responsabilità e delle linee di dipendenza gerarchica, nonché della coerenza tra le attività effettivamente svolte e quanto previsto nell'organigramma aziendale.
- **Procedure operative** – L'attenzione è stata rivolta alla verifica dell'esistenza di procedure formalizzate per regolamentare le attività svolte nelle aree a rischio, considerando sia le fasi negoziali, sia quelle di istruzione e formazione delle decisioni

aziendali. È stata inoltre ricostruita la prassi operativa per individuare le fasi procedimentali e i punti di controllo da inserire o migliorare.

- **Sistema autorizzativo** – L'analisi ha riguardato l'esistenza di poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate o effettivamente esercitate. La verifica è stata condotta mediante l'esame delle procure e delle deleghe interne, in coerenza con l'organigramma aziendale.
- **Principi etici formalizzati** – È stata effettuata una revisione e una formalizzazione più chiara e completa dei principi etici della Società.

Sulla base di tali criteri, sia con riferimento al sistema di controllo preventivo sia agli ulteriori elementi del sistema di controllo (procedure operative, principi etici, formazione del personale, sistema disciplinare), sono state avviate le azioni migliorative ritenute necessarie.

3.5 Finalità del Modello

Il presente Modello è finalizzato alla:

a) prevenzione della commissione di uno dei reati di cui al Decreto 231/2001;

b) promozione e valorizzazione in misura ancora maggiore di una cultura etica al proprio interno, in un'ottica di correttezza e trasparenza nella conduzione degli affari;

c) determinazione in tutti coloro che operano in nome e per conto di Neverhack Italy, della consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;

d) determinazione della consapevolezza che tali forme di comportamento illecito sono fortemente condannate da Neverhack Italy in quanto (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono, comunque, contrarie alle disposizioni di legge e ai principi etico-sociali cui la società intende attenersi nell'espletamento della propria missione aziendale;

e) introduzione di un meccanismo che consenta di istituire un processo permanente di analisi delle attività aziendali, volto a individuare le aree nel cui ambito possano astrattamente configurarsi i reati indicati dal Decreto;

f) introduzione di principi di controllo a cui il sistema organizzativo debba conformarsi così da poter prevenire, nel concreto, il rischio di commissione dei reati indicati dal Decreto nelle specifiche attività potenzialmente a rischio reato;

g) introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto dei suddetti principi di controllo e, in particolare, delle misure indicate nel presente Modello;

h) istituzione dell'Organismo di Vigilanza con il compito di vigilare sul corretto funzionamento e l'osservanza del Modello e di curarne il suo aggiornamento.

3.6 Le parti del Modello

Il Modello di Neverhack Italy è composto da una Parte Generale e da una Parte Speciale.

Nell'ambito della Parte Speciale, per ciascuna sezione dedicata alle diverse categorie di reato presupposto, sono indicati:

- le aree ritenute a rischio di reato;
- le funzioni, i servizi e/o gli uffici aziendali che operano nelle aree a rischio o nell'ambito delle attività sensibili;
- le attività sensibili;
- i reati astrattamente perpetrabili;
- esempi di possibili modalità di realizzazione del reato e delle relative finalità;
- la tipologia dei controlli chiave ritenuti necessari con riferimento a ciascuna attività a rischio o strumentale. L'individuazione dei controlli necessari per garantire l'attuazione dei principi codificati nel D.Lgs. n. 231/2001 è avvenuta:
    1. attraverso l'analisi concreta della realtà aziendale, volta a comprendere le procedure sottese ai processi decisionali sensibili o strumentali;
    2. attraverso l'implementazione delle procedure già esistenti, ritenuta necessaria per assicurare il rispetto dei principi di trasparenza, segregazione delle funzioni e adeguati flussi informativi verso l'Organismo di Vigilanza;
- il sistema autorizzativo e di segregazione delle funzioni;
- la tracciabilità (e archiviazione) delle attività.

Costituiscono, inoltre, parte integrante del Modello:

- il Codice Etico di Neverhack Italy, contenente i principi ispiratori della Società;
- il sistema disciplinare, che prevede le sanzioni applicabili in caso di inosservanza del Modello;
- il Regolamento dell'Organismo di Vigilanza;
- la Procedura "Gestione Whistleblowing", adottata in applicazione del D.Lgs. n. 24/2023.

3.7 Destinatari del Modello

Le regole contenute nel presente Modello si applicano a tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo in Neverhack Italy, ai dipendenti, nonché ai consulenti, collaboratori, agenti, procuratori e, in generale, a tutti i terzi che agiscono per conto della Società nell'ambito delle attività considerate "a rischio reato", in forza di apposita clausola di assoggettamento al Modello.

I destinatari del Modello sono pertanto tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza derivanti dai rapporti giuridici instaurati con la Società.

Nei confronti di tali soggetti, la Società adotta specifiche clausole contrattuali volte a richiamare il rispetto dei principi del Modello e del Codice Etico, nonché a prevedere obblighi di cooperazione con l'Organismo di Vigilanza, facoltà di audit e adeguati rimedi contrattuali, inclusa la risoluzione del rapporto in caso di violazioni rilevanti.

3.8 Approvazione e modifica del Modello

L'approvazione del Modello costituisce prerogativa e responsabilità esclusiva del Consiglio di Amministrazione di Neverhack Italy, così come la formulazione di eventuali modifiche e integrazioni sia ai documenti che compongono il MOGC che alla mappatura delle aree a rischio, anche su segnalazione dell'Organismo di Vigilanza.

Le procedure operative rappresentano elementi di controllo delle attività sensibili individuate a seguito della mappatura delle aree a rischio. Ogni ipotesi o proposta di integrazione o modifica delle procedure del Modello deve, pertanto, essere comunicata anche all'Organismo di Vigilanza.

3.9 Attuazione del Modello

L'attuazione del presente Modello è un processo dinamico che ha inizio con la sua approvazione da parte del Consiglio di Amministrazione.

Per la fase di attuazione, il CdA — supportato dall'Organismo di Vigilanza nei limiti dei compiti a quest'ultimo attribuiti — è responsabile, ciascuno per il proprio ambito di competenza, dell'implementazione dei vari elementi del Modello, incluse le procedure organizzative.

In ogni caso, Neverhack Italy S.p.A. ribadisce che la corretta attuazione e il rispetto delle disposizioni aziendali, e quindi delle regole contenute nel presente Modello, costituiscono un obbligo per tutto il personale. In particolare, ciascun esponente aziendale è responsabile, nell'ambito delle proprie competenze, del controllo primario sulle attività svolte, con specifica attenzione a quelle a rischio.

4 Gli elementi del Modello

4.1 Protocollo descrittivo del processo di mappatura delle aree a rischio e dei controlli

L'art. 6, comma 2, lett. a), del Decreto prevede che il Modello debba includere un meccanismo volto a "individuare le attività nel cui ambito possono essere commessi reati".

L'identificazione degli ambiti nei quali può sussistere il rischio di commissione dei reati richiede una valutazione approfondita di tutti i processi aziendali, finalizzata a verificare l'astratta configurabilità delle fattispecie di reato previste dal Decreto e l'idoneità degli elementi di controllo esistenti a prevenirne la realizzazione. Da tale analisi deriva un documento aziendale denominato "mappatura delle aree a rischio", che costituisce presupposto fondamentale e parte integrante del presente Modello, determinando l'ambito di efficacia e operatività di tutti i suoi elementi costitutivi.

Successivamente, i risultati dell'attività di mappatura delle aree a rischio e dei relativi controlli devono essere aggiornati dal management aziendale, su impulso dell'Organismo di Vigilanza, anche con il supporto di professionisti esperti nelle tecniche di mappatura. Tali aggiornamenti devono essere effettuati ogniqualvolta si verifichino modifiche sostanziali nella struttura organizzativa della Società (ad esempio, costituzione o modifica di unità organizzative, avvio o variazione di attività di Neverhack), oppure in caso di rilevanti modifiche legislative (come l'introduzione di nuove fattispecie di reato rilevanti ai fini del Decreto).

I risultati delle verifiche periodiche sulla mappatura delle aree a rischio e sui relativi controlli sono oggetto di una specifica comunicazione semestrale da parte dell'Organismo di Vigilanza al Consiglio di Amministrazione, che provvede ad adottare le opportune delibere in merito all'aggiornamento del Modello.

4.2 Principi di controllo

La Società ha previsto un sistema di controlli incentrato sui principi di seguito rappresentati, così come peraltro previsto nelle Linee Guida di Confindustria.

Si premette, al riguardo, che nell'ambito di ciascuna sezione della parte speciale del Modello sono state anzitutto evidenziate le regole generali trasversali a tutti i processi aziendali rilevanti, ossia i principi generali di comportamento cui deve uniformarsi la condotta degli esponenti aziendali nel settore di interesse (ad es., correttezza e trasparenza nella gestione dei rapporti con la Pubblica Amministrazione, gestione degli stessi riservata ai soggetti aziendali autorizzati).

I principi di controllo, che dovranno essere assicurati in tutte le attività "a rischio reato", consistono nel:

- garantire integrità ed etica nello svolgimento dell'attività, tramite la previsione di opportune regole di comportamento volte a disciplinare ogni specifica attività considerata a rischio (per esempio nei rapporti con la P.A.);
- definire formalmente i compiti, le responsabilità di ciascun esponente aziendale coinvolto nelle attività a rischio;
- attribuire le responsabilità decisionali in modo commisurato al grado di responsabilità e autorità conferito;
- definire, assegnare e comunicare correttamente i poteri autorizzativi e di firma, prevedendo, quando richiesto, una puntuale indicazione delle soglie di approvazione delle spese in modo tale che a nessun soggetto siano attribuiti poteri discrezionali illimitati;
- garantire il principio di separazione dei ruoli nella gestione dei processi, provvedendo ad assegnare a soggetti diversi le fasi cruciali di cui si compone il processo e, in particolare, quella dell'autorizzazione, dell'esecuzione e del controllo;
- regolamentare l'attività a rischio, per esempio tramite apposite procedure, prevedendo gli opportuni punti di controllo (verifiche, riconciliazioni, quadrature, meccanismi informativi, ecc.);

- assicurare la verificabilità, la documentabilità, la coerenza e la congruità di ogni operazione o transazione. A tal fine, deve essere garantita la tracciabilità dell'attività attraverso un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli. È opportuno, dunque, che per ogni operazione si possa facilmente individuare chi abbia autorizzato l'operazione, chi l'abbia materialmente effettuata, chi abbia provveduto alla sua registrazione e chi abbia effettuato un controllo sulla stessa. La tracciabilità delle operazioni è assicurata con un livello maggiore di certezza dall'utilizzo di sistemi informatici molto avanzati in grado di gestire l'operazione consentendo il rispetto dei requisiti sopra descritti;
- assicurare la documentabilità dei controlli effettuati. A tal fine le procedure con cui vengono attuati i controlli devono garantire la possibilità di ripercorrere le attività di controllo effettuate, in modo tale da consentire la valutazione circa la coerenza delle metodologie adottate e la correttezza dei risultati emersi;
- garantire la presenza di appositi meccanismi di *reporting* che consentano la sistematica rendicontazione da parte del personale che svolge l'attività considerata a rischio (report scritti, relazioni, ecc.);
- garantire l'affidabilità del reporting finanziario al vertice aziendale;
- prevedere momenti di controllo e monitoraggio sulla correttezza dell'attività svolta dalle singole funzioni nell'ambito del processo considerato (rispetto delle regole, corretto utilizzo dei poteri di firma e di spesa, ecc.).

In relazione a ciascuna area a rischio reato o strumentale sono individuate le modalità attraverso le quali i controlli fondamentali sopra descritti vengono declinati e attuati in conformità alle procedure aziendali.

I precetti sopra descritti devono essere rispettati in tutti i processi aziendali e, in particolar modo, nei processi individuati come sensibili.

Sarà responsabilità dell'OdV verificare che gli esponenti aziendali competenti provvedano tempestivamente alla verifica e adeguamento dei propri processi ai principi sopra riportati.

L'esito di detto processo di verifica e adeguamento dovrà essere oggetto di specifico *report* periodico da parte degli esponenti aziendali, per quanto di loro competenza, secondo la modalità e la tempistica stabilite dall'OdV stesso.

L'Organismo di Vigilanza svolge esclusivamente funzioni di vigilanza, controllo e monitoraggio sull'efficace attuazione del Modello e non esercita attività di gestione operativa, né assume decisioni in luogo delle funzioni aziendali competenti.

Restano in capo alle singole funzioni aziendali le responsabilità operative e i controlli di primo livello relativi ai processi di rispettiva competenza.

4.3 Il sistema procedurale

In attuazione dei principi sopra descritti, Neverhack Italy S.p.A. ha implementato il sistema procedurale volto a regolamentare i principali processi aziendali in ottemperanza a quanto richiesto dal D.Lgs. n. 231/2001.

Tale sistema, che costituisce parte integrante del Modello ed è compendiato, per quanto di interesse, nella Parte Speciale, prevede un insieme di procedure aziendali organizzate secondo criteri di codifica in grado di identificare le procedure adottate, allo scopo di prevenire e impedire la commissione dei reati previsti dal Decreto.

4.4 Protocollo per l'adozione e l'aggiornamento del Codice Etico

In ottemperanza ai criteri di buona *governance*, Neverhack Italy ha adottato il Codice Etico con l'obiettivo di garantire il rispetto di determinati principi e regole di condotta che contribuiscono alla prevenzione dei reati previsti dal D.Lgs. n. 231/2001.

La Società garantisce un'ampia diffusione del Codice Etico, tale da assicurarne la conoscenza a tutti i destinatari.

Ogni eventuale modifica del Codice Etico è di competenza del Consiglio di Amministrazione.

Il Codice Etico si rivolge sia ai soggetti legati direttamente da un rapporto di lavoro dipendente, dai quali Neverhack può esigere il rispetto delle disposizioni etiche, sia agli esponenti aziendali, consulenti, collaboratori, agenti, procuratori e terzi, che possono svolgere attività per conto della Società.

Il Codice Etico, pertanto, si applica direttamente anche ai soggetti nei cui confronti il rispetto dei principi etici può essere contrattualmente previsto. Nei contratti che regolano il rapporto con tali soggetti è inserita apposita clausola che richiama l'obbligo di conformarsi ai principi etici, in considerazione delle attività aziendali potenzialmente esposte al rischio di commissione dei reati.

L'Organismo di Vigilanza è incaricato di verificare il funzionamento e l'osservanza del Codice Etico in relazione alle attività specifiche della Società, provvedendo a comunicare tempestivamente all'Amministratore Delegato ogni eventuale incoerenza o esigenza di aggiornamento emersa dalle attività svolte o dalle segnalazioni ricevute.

Eventuali dubbi sull'applicazione dei principi e delle regole contenute nel Codice Etico devono essere tempestivamente sottoposti all'Organismo di Vigilanza. Allo stesso modo, chiunque venga a conoscenza di violazioni dei principi del Codice Etico o di fatti che possano comprometterne la portata o l'efficacia è tenuto a darne immediata segnalazione all'Organismo di Vigilanza. In ogni caso, l'Organismo di Vigilanza non fornisce pareri o consulenza alla Società, in coerenza con la necessaria terzietà e imparzialità.

Nel caso in cui una delle disposizioni del Codice Etico dovesse entrare in conflitto con disposizioni previste nei regolamenti interni o nelle procedure, prevarrà quanto stabilito dal Codice.

4.5 Il sistema di gestione delle risorse finanziarie

L'art. 6, comma 2, lett. c), del Decreto dispone che i modelli devono prevedere "modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati". La disposizione trova la sua *ratio* nella constatazione che la maggior parte dei reati di cui al D.Lgs. n. 231/2001 può essere attuata tramite le risorse finanziarie delle società (per esempio, la costituzione di fondi extra-contabili per la realizzazione di atti di corruzione).

Le Linee Guida raccomandano l'adozione di meccanismi di procedimentalizzazione delle decisioni, che, rendendo documentate e verificabili le varie fasi del processo decisionale, impediscano la gestione impropria delle risorse finanziarie dell'ente.

Per assicurare la corretta gestione delle risorse finanziarie, Neverhack Italy ha provveduto a regolamentare i principali processi amministrativo-contabili con specifiche procedure organizzative.

Dette procedure costituiscono parte integrante del presente Modello e la violazione fraudolenta delle regole in esse previste costituisce motivo per l'applicazione delle sanzioni previste dal Sistema disciplinare.

Sulle procedure sopra richiamate deve essere esercitato un adeguato controllo da parte di tutti gli esponenti aziendali coinvolti nei processi di gestione delle risorse finanziarie, in conformità al principio di responsabilizzazione delle funzioni, nonché da parte degli organi e delle funzioni di controllo di Neverhack. Tra questi, l'Organismo di Vigilanza è tenuto a rendicontare, nelle proprie comunicazioni periodiche al Consiglio di Amministrazione, i controlli effettuati in merito alla conoscenza e alla corretta applicazione delle suddette procedure.

Ogni modifica alle suddette procedure dovrà essere comunicata all'Organismo di Vigilanza, affinché possa svolgere gli adempimenti di propria competenza necessari a garantire la corretta attuazione del presente Modello.

4.6 Il sistema disciplinare

Il sistema sanzionatorio del presente Modello è un sistema autonomo di sanzioni finalizzato a rafforzare il rispetto e l'efficace attuazione del Modello in conformità a quanto previsto dall'articolo 6, comma 2, lettera e), del Decreto.

L'applicazione delle misure sanzionatorie stabilite dal Modello non sostituisce eventuali ulteriori sanzioni di diversa natura (penale, amministrativa, civile e tributaria) che possano derivare dal medesimo fatto di reato.

L'applicazione delle sanzioni disciplinari prescinde dalla instaurazione e dall'esito di eventuale procedimento penale avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del Decreto.

Ogni violazione del Modello o delle procedure stabilite in attuazione dello stesso, da chiunque commessa, deve essere tempestivamente comunicata, per iscritto, all'Organismo di Vigilanza (cfr. cap. 4), ferme restando le procedure e i provvedimenti di competenza del titolare del potere disciplinare.

Il dovere di segnalazione grava su tutti i destinatari del presente Modello.

Ricevuta la segnalazione, l'Organismo di Vigilanza avvia immediatamente i necessari accertamenti, garantendo la riservatezza del soggetto interessato. Le sanzioni per le violazioni delle disposizioni del presente Modello sono adottate dall'Amministratore Delegato. Una volta valutata la violazione, l'Organismo di Vigilanza informa tempestivamente l'Amministratore Delegato, che avvia il procedimento disciplinare di propria competenza, provvedendo alle contestazioni e all'eventuale applicazione delle sanzioni.

Costituiscono infrazioni disciplinari i seguenti comportamenti:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, dei principi e delle procedure previste dal presente Modello o stabilite per la sua attuazione;
- la redazione, eventualmente in concorso con altri, di documentazione non veritiera;
- l'agevolazione, mediante condotta omissiva, della redazione da parte di altri di documentazione non veritiera;
- la sottrazione, la distruzione o l'alterazione della documentazione inerente alla procedura per sottrarsi al sistema dei controlli previsto dal Modello;
- l'ostacolo alla attività di vigilanza dell'OdV;
- l'impedimento all'accesso alle informazioni e alla documentazione richiesta dai soggetti preposti ai controlli delle procedure e delle decisioni;
- l'attuazione di condotte ritorsive, discriminatorie e punitive nei confronti del personale autore di segnalazioni di violazioni del sistema dei controlli previsto dal Modello e/o di illeciti;
- l'abuso del potere/dovere di segnalazione, tramite indicazioni false o infondate sulla commissione di illeciti e/o violazioni del Modello di Organizzazione, Gestione e Controllo;
- la realizzazione di qualsiasi altra condotta idonea a eludere il sistema di controllo previsto dal Modello.

<u>Sanzioni e misure disciplinari</u>

Le sanzioni applicabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché proporzionate alla gravità della violazione valutata alla luce del grado di imprudenza, negligenza, imperizia ovvero intenzionalità della condotta; altresì, alla luce della eventuale reiterazione di comportamenti illeciti, del ruolo e della responsabilità dell'autore, delle mansioni e del grado di autonomia del lavoratore e di ogni altra particolare circostanza del fatto.

Il Modello costituisce un complesso di norme alle quali il personale dipendente deve uniformarsi anche ai sensi di quanto previsto dai rispettivi CCNL in materia di norme comportamentali e di sanzioni disciplinari. Pertanto, la violazione delle previsioni del Modello e delle sue procedure di attuazione comporta l'applicazione del procedimento disciplinare e delle relative sanzioni, ai sensi di legge e dei citati CCNL.

Nei confronti dei lavoratori dipendenti con qualifica di operaio, impiegato e quadro il sistema disciplinare è applicato in conformità all'art. 7 della legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori) e ai vigenti CCNL applicabili. Qualora il fatto costituisca violazione anche di doveri discendenti dalla legge o dal rapporto di lavoro, tali da non consentire la prosecuzione del rapporto di lavoro neppure in via provvisoria, potrà essere deciso il licenziamento senza preavviso, a norma dell'art. 2119 c.c., fermo il rispetto del procedimento disciplinare.

Le altre sanzioni comminabili ai lavoratori dipendenti sono:

- il rimprovero verbale;
- l'ammonizione scritta;
- multa in conformità alle previsioni del CCNL;
- sospensione dal lavoro e dalla retribuzione in conformità alle previsioni del CCNL;
- licenziamento con preavviso.

In ogni caso verranno applicate tutte le disposizioni e le garanzie previste dal CCNL in materia di procedimento disciplinare.

Il rispetto delle disposizioni del Modello vale nell'ambito dei contratti di lavoro di qualsiasi tipologia e natura, inclusi quelli con i Dirigenti, a progetto, part-time, nonché nei contratti di collaborazione rientranti nella c.d. parasubordinazione. Se la violazione riguarda i Dirigenti, il sistema disciplinare è applicato in conformità alla legge e al CCNL applicabile. Attraverso la contestazione può essere disposta la revoca di eventuali procure affidate al soggetto interessato.

Se la violazione riguarda un Amministratore della Società, l'Organismo di Vigilanza deve darne immediata comunicazione all'Assemblea dei Soci.

Nei confronti dell'Amministratore che abbia commesso una violazione del Modello o delle procedure stabilite in attuazione del medesimo, l'Assemblea dei Soci può applicare ogni idoneo provvedimento consentito dalla legge, fra cui le seguenti sanzioni, determinate a seconda della gravità del fatto e della colpa, nonché delle conseguenze che sono derivate alla Società:

a) richiamo formale scritto;

b) sanzione pecuniaria pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;

c) revoca, totale o parziale, della nomina e procura, qualora la violazione dell'amministratore sia tale da ledere la fiducia della Società nei suoi confronti.

In caso di violazione del Modello da parte dell'Organismo di Vigilanza, gli altri membri — qualora l'organo sia collegiale — oppure, in alternativa, l'Amministratore Delegato informano immediatamente l'Assemblea dei Soci, che adotta i conseguenti provvedimenti, tra cui la possibile revoca dell'incarico, previa valutazione delle argomentazioni difensive e/o delle giustificazioni presentate.

Per i soggetti esterni o le controparti contrattuali destinatarie del Modello, l'Organismo di Vigilanza, sentiti i responsabili di funzione competenti in relazione al contratto o al rapporto interessato, propone per ciascuna tipologia di rapporto le misure sanzionatorie applicabili in caso di violazione delle previsioni del Modello o delle procedure adottate per la sua attuazione, individuandone altresì le modalità di applicazione. Qualora si verifichino fatti che possano integrare una violazione del Modello da parte di tali soggetti, l'Organismo di Vigilanza informa l'Amministratore Delegato mediante relazione scritta; quest'ultimo, sentiti i responsabili di funzione competenti, valuterà le modalità con cui procedere all'accertamento della violazione.

4.7 L'Organismo di Vigilanza

Il D.Lgs. n. 231/2001, all'art. 6, comma 1, lett. b), prevede, tra i presupposti indispensabili per l'esonero dalla responsabilità conseguente alla commissione dei reati, l'istituzione di un organismo interno all'Ente – c.d. "Organismo di Vigilanza" (OdV).

Requisiti dell'Organismo di Vigilanza

L'OdV deve soddisfare i seguenti requisiti:

- **Autonomia e indipendenza**. Come anche precisato dalle Linee Guida, la posizione dell'OdV nell'Ente "deve garantire l'autonomia dell'iniziativa di controllo da ogni forma di interferenza e/o condizionamento da parte di qualunque componente dell'Ente" (ivi compreso l'organo dirigente). L'OdV, pertanto, deve essere inserito in una posizione la più elevata possibile con la previsione di un riporto informativo al massimo vertice operativo aziendale. Inoltre, per garantirne la necessaria autonomia di iniziativa e indipendenza, "è indispensabile che all'OdV non siano attribuiti compiti operativi che, rendendolo partecipe di decisioni e attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello".

- **Professionalità**. Tale requisito si riferisce alle competenze tecniche specialistiche di cui deve essere dotato l'OdV per poter svolgere l'attività che la norma gli attribuisce. In particolare, il componente dell'OdV deve avere conoscenze specifiche in relazione a qualsiasi tecnica utile per compiere l'attività ispettiva, di consulenza, di analisi del sistema di controllo e di tipo giuridico (in particolare nel settore penalistico e societario), come chiaramente specificato nelle Linee Guida. È infatti essenziale la conoscenza delle tecniche di analisi e valutazione dei rischi, del *flow charting* di procedure e processi, delle metodologie per l'individuazione di frodi, del campionamento statistico e della struttura e delle modalità realizzative dei reati.
- **Continuità di azione**. Tale requisito deve connotare l'attività dell'OdV per garantire l'efficace attuazione del Modello organizzativo.

Pertanto, quale organo preposto a vigilare sul funzionamento e l'osservanza del Modello e a curarne il continuo aggiornamento, nonché quale organo dotato di specifici poteri di iniziativa e di controllo, l'OdV deve:

- essere indipendente e in posizione di terzietà rispetto a coloro sui quali dovrà effettuare la vigilanza;
- essere dotato di autonomi poteri di iniziativa e di controllo, nei limiti delle proprie competenze;
- essere dotato di autonomia di spesa, con un budget definito annualmente dal CdA;
- essere privo di compiti operativi;
- assicurare continuità d'azione;
- avere i requisiti di professionalità sopra descritti;
- poter usufruire di un canale diretto di comunicazione con i vertici aziendali.

<u>Individuazione dell'Organismo di Vigilanza</u>

In attuazione di quanto previsto dal Decreto e dalle Linee Guida, e nel rispetto dei requisiti di autonomia, indipendenza, professionalità e continuità d'azione sopra richiamati, l'Organismo di Vigilanza di Neverhack Italy è stato individuato in un **organo collegiale composto da tre membri esterni di comprovata esperienza nella materia di cui al D.Lgs. 231/2001**. Alle riunioni dell'Organismo di Vigilanza partecipa stabilmente, in qualità di invitato permanente, il responsabile della funzione Compliance.

Il Regolamento dell'Organismo di Vigilanza, cui si rinvia per quanto non espressamente riportato nel presente documento, disciplina le modalità e i requisiti per la nomina dei suoi componenti, le cause di incompatibilità, le ipotesi di revoca o cessazione del mandato, nonché i compiti e i poteri dell'Organo. Esso definisce inoltre le caratteristiche e le modalità di funzionamento dell'Organismo stesso.

Il componente dell'Organismo di Vigilanza, a garanzia della posizione di terzietà ed autonomia, non deve:

1. intrattenere, direttamente o indirettamente relazioni economiche con la Società, con le sue eventuali Controllate, con gli Amministratori esecutivi, con i soci o con le società che controllano Neverhack, di rilevanza tale da condizionarne l'autonomia di giudizio, valutata anche in relazione alla condizione patrimoniale soggettiva della persona fisica in questione, fermo restando il diritto al compenso e all'eventuale autorizzazione a spese sostenute in ragione dell'incarico;
2. essere titolare, direttamente o indirettamente, di partecipazioni azionarie di entità tale da permettere di esercitare il controllo o un'influenza notevole sulla Società;
3. essere stretto familiare di Amministratori della Società o di soggetti che si trovino nelle situazioni indicate nei punti precedenti.

All'atto dell'accettazione dell'incarico, i componenti dell'Organismo di Vigilanza rilasciano una dichiarazione nella quale attestano l'assenza dei menzionati motivi di incompatibilità.

Inoltre, i componenti dell'Organismo di Vigilanza, per poter essere scelti e mantenere la carica non devono essere stati condannati, nemmeno con sentenza non ancora irrevocabile, per avere commesso uno dei reati di cui al D.Lgs. n. 231/2001 ovvero a una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o dagli uffici direttivi delle persone giuridiche.

I componenti dell'Organismo di Vigilanza durano in carica il periodo stabilito in sede di nomina e possono essere rieletti, previa verifica esplicita del permanere dei requisiti di eleggibilità sopra descritti. I componenti dell'Organismo di Vigilanza possono essere revocati soltanto dal Consiglio di Amministrazione in caso di:

1. sopravvenienza di una delle cause di incompatibilità di cui sopra;
2. inadempienza reiterata ai compiti previsti dal Modello;
3. inattività ingiustificata che abbia comportato l'applicazione di sanzioni interdittive per la Società.

Ciascun componente dell'Organismo di Vigilanza può rassegnare in qualunque momento le proprie dimissioni e cessa dall'incarico nel momento in cui tali dimissioni vengano accettate dal Consiglio di Amministrazione, ovvero venga nominato altro componente in sostituzione. In ogni caso dopo un mese dalle dimissioni cessa dalla carica.

L'OdV e l'interazione con gli altri esponenti aziendali**.**

L'OdV, nello svolgimento dei compiti affidatigli e per le proprie finalità istituzionali, potrà avvalersi inoltre della collaborazione:

1. di altre unità organizzative della Società;
2. di opportuni supporti esterni, secondo le valutazioni del caso.

È previsto, inoltre, per il corretto e completo espletamento delle attività di vigilanza, un coordinamento sistematico dell'OdV con le risorse della Società.

Il sistema dei flussi informativi da parte dell'Organismo di Vigilanza.

L'Organismo di Vigilanza riferisce annualmente all'Amministratore Delegato e al Consiglio di Amministrazione in merito all'attuazione del Modello e alle eventuali criticità emerse.

In particolare, l'attività di *reporting* ha per oggetto:

- l'attività complessivamente svolta nel corso del periodo, con particolare riferimento a quella di verifica;
- le eventuali criticità emerse sia in termini di comportamenti o eventi interni alla Società, sia in termini di efficacia del Modello;
- i necessari e/o opportuni interventi correttivi e migliorativi del Modello ed il loro stato di realizzazione;
- l'accertamento di comportamenti non in linea con il Modello o con il Codice Etico;
- la rilevazione di carenze organizzative o procedurali tali da esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto;
- l'eventuale mancata o carente collaborazione da parte delle funzioni aziendali nell'espletamento dei propri compiti ovvero nell'inoltro della reportistica di competenza;
- il rendiconto delle spese sostenute;
- eventuali mutamenti normativi che richiedono l'aggiornamento del Modello;

- qualsiasi informazione ritenuta utile ai fini dell'assunzione delle determinazioni urgenti;
- le attività cui non si è potuto procedere per giustificate ragioni di tempo e risorse.

L'OdV si riunisce con cadenza almeno trimestrale e relaziona su base periodica con l'Amministratore Delegato e annualmente al Consiglio di Amministrazione.

Gli incontri con gli organi societari cui l'OdV riferisce sono preferibilmente verbalizzati e copia dei verbali è custodita dall'OdV stesso nell'apposito archivio secondo le modalità e i tempi da questo stabiliti.

L'Organismo di Vigilanza può essere convocato in qualsiasi momento dal Consiglio di Amministrazione o dall'Assemblea dei Soci e può, a sua volta, richiedere di essere convocato per riferire in merito al funzionamento del Modello e a specifiche situazioni direttamente o indirettamente connesse alla sua applicazione e/o all'attuazione del Decreto.

L'OdV, inoltre, si relaziona periodicamente con gli altri organi di controllo (Collegio Sindacale e Revisore).

Il sistema dei flussi informativi nei confronti dell'Organismo di Vigilanza.

L'art. 6, comma 2, lett. d), del D.Lgs. n. 231/01 impone la previsione nel Modello di obblighi informativi nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello stesso.

L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto.

Le informazioni fornite all'OdV mirano a migliorare le sue attività di pianificazione dei controlli e comportano un'attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati.

In particolare, oltre alle informazioni specificatamente richieste nelle procedure aziendali, devono essere tempestivamente trasmessi all'OdV, in via esclusiva e riservata, da parte di tutti gli esponenti aziendali le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto, avviate anche nei confronti di ignoti;
- ogni violazione del Modello e dei suoi elementi costitutivi e ogni altro aspetto potenzialmente rilevante ai fini dell'applicazione del Decreto;

- eventi e atti che possano ledere la garanzia di tutela dell'integrità dei lavoratori e ogni altro aspetto in tema di misure antinfortunistiche e di salute e igiene sul lavoro potenzialmente rilevante ai fini dell'applicazione dell'art. 25 *septies* del D.Lgs. n. 231/2001;
- rapporti predisposti dagli esponenti aziendali e dagli altri organi di controllo nell'ambito delle attività di controllo svolte, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del sistema disciplinare, evidenzianti i procedimenti disciplinari svolti e le eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti nei confronti dei dipendenti), ovvero i provvedimenti motivati di archiviazione dei procedimenti disciplinari;
- ogni eventuale modifica e/o integrazione al sistema di deleghe e procure;
- esistenza di attività aziendali risultate e/o percepite come prive in tutto o in parte di apposita e/o adeguata regolamentazione (assenza totale o parziale di specifica regolamentazione, inadeguatezza dei principi del Codice Etico e/o delle procedure operative rispetto alle finalità cui sono preordinati, sotto il profilo della chiarezza e comprensibilità, aggiornamento e corretta comunicazione, ecc.);
- ogni eventuale emanazione, modifica e/o integrazione effettuata o ritenuta necessaria alle procedure operative concernenti il Modello e il Codice Etico.

Oltre al delineato sistema informativo, che assume valore tassativo, chiunque venga in possesso di notizie relative alla commissione di reati o a comportamenti ritenuti non in linea con quanto previsto dal presente Modello è tenuto comunque a darne immediata notizia all'Organismo di Vigilanza.

4.8 Whistleblowing

La Società, al fine di agevolare le segnalazioni da parte dei soggetti che vengano a conoscenza di violazioni, anche potenziali, del Modello, ha adottato un'apposita procedura in conformità al D.Lgs. n. 24/2023 ("**Procedura Gestione Whistleblowing**"), attivando specifici canali informatici dedicati, tra cui una piattaforma "*Whistleblowing*" accessibile dal sito web aziendale.

Le segnalazioni effettuate secondo tale procedura — che costituisce modalità di comunicazione alternativa rispetto ai flussi diretti all'Organismo di Vigilanza — sono indirizzate al c.d. Gestore delle Segnalazioni, individuato dalla Società nell'Organismo di Vigilanza, congiuntamente alla funzione Legal.

Il Gestore delle Segnalazioni opera garantendo la tutela dei segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza della loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti di Neverhack Italy e delle persone coinvolte, nonché della reputazione del/dei segnalato/i.

Saranno applicate adeguate sanzioni nei confronti di coloro che, all'interno dell'azienda, attuino comportamenti ritorsivi, discriminatori o vessatori nei confronti degli autori di segnalazioni di illeciti.

È altresì vietato ai dipendenti formulare segnalazioni false o infondate, abusando del diritto di segnalazione loro riconosciuto.

Saranno parimenti applicate sanzioni nei confronti di coloro che, abusando del potere o dovere di segnalazione, forniscano indicazioni false o infondate in merito alla commissione di illeciti e/o violazioni del Modello di Organizzazione, Gestione e Controllo.

4.9 Piano di formazione e comunicazione

La formazione interna costituisce uno strumento imprescindibile per un'efficace implementazione del Modello e per una diffusione capillare dei principi di comportamento e di controllo adottati da Neverhack Italy per la prevenzione dei reati di cui al D.Lgs. n. 231/2001.

A tal fine, la Società promuove la realizzazione di un piano di formazione specifico dei soggetti destinatari del presente Modello, in merito ai contenuti di tale documento e del Decreto.

La partecipazione alle attività formative in materia di D.Lgs. n. 231/2001 e Modello è obbligatoria per tutti i destinatari, secondo le modalità e i livelli di approfondimento definiti in funzione del ruolo ricoperto.

Le attività formative sono tracciate e documentate; la Società prevede strumenti di verifica dell'apprendimento e meccanismi di gestione dei casi di mancata partecipazione.

I requisiti che detto programma di formazione deve rispettare sono i seguenti:

- adeguatezza alla posizione organizzativa dei destinatari (neoassunti, impiegati, quadri, dirigenti, ecc.);
- differenziazione dei contenuti in funzione dell'attività svolta dal soggetto all'interno dell'azienda (attività a rischio, attività di controllo, attività non a rischio, ecc.);
- periodicità modulata in base al grado di cambiamento dell'ambiente esterno in cui opera la Società e alla capacità di apprendimento del personale;
- qualificazione del relatore, che deve essere persona competente e autorevole, in grado di garantire la qualità dei contenuti e di evidenziare l'importanza della formazione per Neverhack e per le strategie aziendali, anche in materia di anticorruzione;
- obbligatorietà della partecipazione.

La formazione può essere classificata in generale o specifica. In particolare, la formazione generale deve interessare tutti i livelli dell'organizzazione per consentire a ogni individuo di:

- conoscere i precetti stabiliti dal D.Lgs. n. 231/2001 e di essere consapevole che Neverhack intende farli propri e renderli parte integrante della cultura aziendale;
- conoscere gli obiettivi che la Società si prefigge di raggiungere tramite l'implementazione del Modello e le modalità con le quali le mansioni di ciascuno possono contribuire al raggiungimento degli stessi;
- avere cognizione del proprio ruolo e delle proprie responsabilità all'interno del sistema di controllo interno presente in Neverhack;
- conoscere quali sono i comportamenti attesi o accettabili e quelli ritenuti non accettabili da Neverhack;
- conoscere i precetti e le tutele previste dalla normativa in materia di whistleblowing ed i canali di *reporting* adeguati al tipo di informazione che si vuole comunicare;
- essere consapevole dei provvedimenti disciplinari applicabili nel caso di violazioni delle regole del presente Modello;
- conoscere i poteri e i compiti dell'OdV e, in conseguenza, gli obblighi informativi nei confronti di tale organismo.

La formazione specifica, invece, interessa tutti quei soggetti che per via della loro attività necessitano di specifiche competenze per gestire le peculiarità dell'attività stessa, come il personale che opera nell'ambito di attività segnalate come potenzialmente "a rischio reato".

Questi dovranno essere destinatari di una formazione sia generale che specifica. In particolare, la formazione specifica dovrà consentire al soggetto di:

- avere consapevolezza dei potenziali rischi associabili alla propria attività, nonché degli specifici meccanismi di controllo da attivare al fine di monitorare l'attività stessa;
- conoscere le tecniche di valutazione dei rischi inerenti all'attività da esso svolta nonché le esatte modalità di svolgimento della stessa e/o le procedure che la regolamentano, per acquisire la capacità di individuare eventuali anomalie e segnalarle nei modi e nei tempi utili per l'implementazione di possibili azioni correttive.

Anche i soggetti preposti al controllo interno, cui spetta il monitoraggio delle attività risultate potenzialmente a rischio, saranno destinatari di una formazione specifica per renderli consapevoli delle loro responsabilità e del loro ruolo all'interno del sistema del controllo interno, nonché delle sanzioni cui vanno incontro nel caso disattendano tali responsabilità e tale ruolo.

In caso di modifiche e/o aggiornamenti rilevanti del Modello saranno organizzati moduli di approfondimento mirati alla conoscenza delle variazioni intervenute.

4.10 Comunicazione del Modello

In linea con quanto previsto dal Decreto e dalle Linee Guida, Neverhack assicurerà la piena diffusione del presente Modello, al fine di garantire che tutto il personale sia adeguatamente informato sui suoi contenuti.

La comunicazione dovrà essere capillare, efficace, chiara e dettagliata, con aggiornamenti periodici connessi ai mutamenti del Modello.

Per essere efficace, la comunicazione deve:

- essere sufficientemente dettagliata in rapporto al livello gerarchico di destinazione;
- utilizzare i canali di comunicazione più appropriati e facilmente accessibili ai destinatari della comunicazione per fornire le informazioni in tempi utili, permettendo al personale destinatario di usufruire della comunicazione stessa in modo efficace ed efficiente;
- essere di qualità in termini di contenuti (tale da rendere fruibili tutte le informazioni necessarie), di tempestività, di aggiornamento (deve contenere l'informazione più recente) e di accessibilità.

Pertanto, il piano effettivo di comunicazione relativo alle componenti essenziali del presente Modello dovrà essere sviluppato, in coerenza ai principi sopra definiti, tramite i mezzi di comunicazione aziendali ritenuti più idonei, quali per esempio la pubblicazione sulle apposite *repository* aziendali e la pubblicazione sul sito internet

4.11 Informativa ai collaboratori esterni e ai partner

Neverhack Italy promuove la conoscenza e l'osservanza dei principi e delle regole di condotta previsti dal Codice Etico e dal presente Modello anche tra i consulenti, i partner, i collaboratori a vario titolo, i clienti e i fornitori. Per tali soggetti, pertanto, saranno predisposti meccanismi per l'inserimento e l'accettazione di clausole contrattuali specifiche che sono inserite negli schemi contrattuali di riferimento. Inoltre, i documenti saranno accessibili sul sito internet.

* * *

ALLEGATI:

1) Elenco Reati presupposto;
2) Mappatura delle aree a rischio;
3) Codice Etico;
4) Regolamento dell'Organismo di Vigilanza;
5) Elenco delle procedure adottate da Neverhack Italy;
6) Procedura "Gestione Whistleblowing".