MODELLO DI ORGANIZZAZIONE,

GESTIONE E CONTROLLO

AI SENSI DELL'ART. 6 DEL D.LGS. 8 GIUGNO 2001, N. 231

Adottato con delibera del Consiglio di Amministrazione del 27/02/2023

Sommario

PARTE GENERALE

PREMESSA

Il presente documento, corredato di tutti i suoi allegati, rappresenta il Modello di Organizzazione, Gestione e Controllo adottato ai sensi del Decreto Legislativo 8 giugno 2001 n. 231 (d'ora in avanti "**D. Lgs. 231/2001**" o "**Decreto**") dalla Società Security Lab S.r.l. (di seguito anche "**Security Lab**" o la "**Società**") e approvato dal Consiglio di Amministrazione della Società stessa.

Security Lab ha riassunto le risultanze dell'attività di valutazione del proprio sistema di controllo interno e gli eventuali correttivi ad esso apportati nel presente Modello di organizzazione, gestione e controllo, alla luce dei principi indicati dal D. Lgs. n. 231 del 2001 e dalle Linee Guida emanate in materia da Confindustria.

DEFINIZIONI

- *Attività Sensibili*: *sono* le attività/processi di Security Lab nel cui ambito sussiste il rischio potenziale di commissione di reati di cui al Decreto;
- *Attività Strumentali*: sono le attività/processi di Security Lab che risultano potenzialmente strumentali alla commissione dei reati di cui al Decreto;
- *Consulenti*: sono i soggetti che, in ragione delle competenze professionali in loro possesso, prestano la propria opera intellettuale in favore o per conto di Security Lab;
- *D.Lgs. 231/2001 o Decreto*: il Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche e integrazioni;
- *Destinatari*: sono tutti i soggetti che, in forza dei rapporti intrattenuti con la Società, sono tenuti all'osservanza del Modello, inclusi: gli amministratori e tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione e controllo sulla stessa o sue unità operative o funzionali, i dipendenti, i collaboratori, gli agenti, i procacciatori e i distributori, i consulenti e quei soggetti che agiscono nell'interesse della Società in quanto legati alla stessa da rapporti giuridici contrattuali o da accordi di altra natura;
- *Dipendenti*: sono i soggetti legati a Security Lab da un contratto di lavoro subordinato;
- *DVR:* Documento di Valutazione dei Rischi ai sensi del D.Lgs. 9 aprile 2008 n. 81;
- *Incaricato di un pubblico servizio*: colui che "*a qualunque titolo presta un pubblico servizio*", intendendosi con pubblico servizio un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa (art. 358 c.p.);
- *Linee Guida Confindustria*: documento di Confindustria, approvato il 7 marzo 2002, successivamente aggiornato il 31 marzo 2008, nel marzo 2014 e, da ultimo, nel giugno 2021, per la costruzione dei Modelli di Organizzazione, Gestione e Controllo di cui al Decreto;
- *Modello*: Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
- *Organismo di Vigilanza o O.d.V.*: Organismo previsto dall'art. 6 del Decreto, preposto alla verifica sul funzionamento e sull'osservanza del Modello;
- *P.A.:* la Pubblica Amministrazione, il Pubblico Ufficiale o l'Incaricato di pubblico servizio;
- *Partner o Collaboratori esterni*: sono le controparti contrattuali di Security Lab, persone fisiche o giuridiche, con cui la Società addivenga ad una qualunque forma di collaborazione contrattualmente regolata;

- *CdA.*: il Consiglio di Amministrazione della Società;
- *Presente documento*: Modello di Organizzazione, Gestione e Controllo della Società;
- *Pubblico Ufficiale*: colui che "*esercita una pubblica funzione legislativa, giudiziaria o amministrativa*" (art. 357 c.p.);
- *Reati o Reati presupposto*: sono le fattispecie di reato alle quali si applica la disciplina prevista dal D.Lgs. 231/2001, anche a seguito di sue successive modifiche o integrazioni;
- *Soggetti Apicali*: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione o il controllo della Società;
- *Soggetti Subordinati*: persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al punto precedente.

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

1.1 Caratteristiche e natura della responsabilità degli Enti

Il Decreto Legislativo 8 giugno 2001 n. 231 (di seguito anche il "**D. Lgs. 231/2001**" o il "**Decreto**"), recante la Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e di altre strutture associative, anche prive di personalità giuridica ("**Enti**"), ha introdotto per la prima volta nell'ordinamento giuridico italiano una forma di responsabilità amministrativa da reato a carico degli Enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

Si tratta di una nuova e più estesa forma di responsabilità, che colpisce l'Ente per i reati commessi, nel suo interesse o vantaggio, da soggetti ad esso funzionalmente legati (soggetti in posizione apicale e soggetti sottoposti alla loro direzione e vigilanza).

1.2 Fattispecie di reato individuate dal Decreto

L'Ente può essere chiamato a rispondere soltanto per i reati espressamente individuati nel Decreto ("**Reati Presupposto**") e non è sanzionabile per altre tipologie di illecito commesso durante lo svolgimento delle proprie attività. Il Decreto indica agli artt. 24 ss. i cosiddetti "*Reati Presupposto*", ovvero gli illeciti da cui può discendere la responsabilità dell'Ente.

Alla data di approvazione del presente documento, i Reati Presupposto rilevanti ai sensi del Decreto appartengono alle seguenti categorie:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- delitti informatici e trattamento illecito di dati (art. 24 bis);
- delitti di criminalità organizzata (art. 24 ter);
- reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis);
- delitti contro l'industria e il commercio (art. 25 bis.1);
- reati societari e corruzione tra privati (art. 25 ter);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater);
- pratiche di mutilazione degli organi genitali femminili (art. 25 quater.1);
- delitti contro la personalità individuale (art. 25 quinquies);

- abuso di mercato (art. 25 sexies);
- omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 septies);
- ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies);
- delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 octies.1);
- delitti in materia di violazione del diritto d'autore (art. 25 novies);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies);
- reati ambientali (art. 25 undecies);
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies);
- razzismo e xenofobia (art. 25 terdecies);
- reati transnazionali (art. 10, L. 146/2006);
- frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati attraverso apparecchi vietati (art. 25 quaterdecies);
- reati tributari (art. 25 quinquesdecies)
- contrabbando (art. 25 sexiesdecies)
- delitti contro il patrimonio culturale (art. 25-septiesdecies)
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies).

Nella consapevolezza che la comprensione delle singole fattispecie sia un presupposto essenziale per l'applicazione del Modello, i Reati Presupposto previsti dal Decreto e dalle leggi speciali ad integrazione dello stesso, sono integralmente richiamati e descritti, con le relative sanzioni, nell'**Allegato A** al presente Modello.

1.3 Criteri di imputazione della responsabilità all'Ente

Nel caso di commissione di uno dei Reati Presupposto, l'Ente è punibile solo nel caso in cui ricorrano determinate condizioni, definite come criteri di imputazione del reato. Tali criteri si distinguono in "oggettivi" e "soggettivi".

a) Il primo criterio oggettivo che deve sussistere ai fini della punibilità dell'Ente è che il reato commesso deve esser compreso tra quelli espressamente indicati come Reati Presupposto nel Decreto.

b) Il secondo criterio oggettivo è che il reato deve essere commesso nell'interesse o a vantaggio dell'Ente. Deve, perciò, essere stato commesso in un ambito inerente le attività specifiche della Società e quest'ultima deve averne tratto un beneficio, anche se solo in maniera potenziale. È sufficiente la sussistenza di almeno una delle due condizioni, alternative tra loro:
   - l'"*interesse*" sussiste quando l'autore del reato ha agito con l'intento di favorire la Società, indipendentemente dalla circostanza che poi tale obiettivo sia stato realmente conseguito;
   - il "*vantaggio*" sussiste quando la Società ha tratto, o avrebbe potuto trarre, dal Reato un risultato positivo, sia esso economico o di altra natura.

La responsabilità dell'Ente sussiste non solo quando esso ha tratto un vantaggio patrimoniale immediato dalla commissione del Reato, ma anche nell'ipotesi in cui, pur nell'assenza di tale risultato, il fatto trovi motivazione nell'interesse dell'Ente. Il miglioramento della propria posizione sul mercato o l'occultamento di una situazione di crisi finanziaria, ad esempio, sono casi che coinvolgono gli interessi dell'Ente senza apportargli però un immediato e diretto vantaggio economico.

c) Il terzo criterio oggettivo è che il Reato Presupposto deve essere stato commesso da uno o più soggetti qualificati, ovvero da *"persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale*" o da coloro che "*esercitano, anche di fatto, la gestione e il controllo"* dell'Ente (soggetti cosiddetti in "*posizione apicale*"), oppure ancora da "*persone sottopose alla direzione e alla vigilanza di uno dei Soggetti Apicali*" (cosiddetti "*subalterni*" o "*subordinati*").

Gli autori del Reato dal quale può derivare una responsabilità amministrativa a carico dell'Ente, quindi, possono essere: (i) soggetti in "*posizione apicale*", quali, ad esempio, il legale rappresentante, l'amministratore o il direttore generale, nonché le persone che esercitano, anche di fatto, la gestione e il controllo dell'Ente e (ii) soggetti "*subalterni*", tipicamente i lavoratori dipendenti, ma anche soggetti esterni all'Ente, ai quali sia stato affidato un incarico da svolgere sotto la direzione e la sorveglianza dei soggetti apicali.

Qualora più soggetti partecipino alla commissione del Reato (ipotesi di concorso di persone nel reato *ex* art. 110 c.p.), non è necessario che il soggetto "*qualificato*" ponga in essere l'azione tipica prevista dalla legge penale. È sufficiente che fornisca un contributo consapevolmente causale alla realizzazione del Reato.

Le disposizioni del Decreto escludono la responsabilità dell'Ente, nel caso in cui questo - prima della commissione del Reato Presupposto - abbia adottato ed efficacemente attuato un "*Modello di organizzazione e di gestione*" idoneo a prevenire la commissione di Reati della specie di quello che è stato realizzato.

La responsabilità dell'Ente, sotto questo profilo, è ricondotta alla "*mancata adozione ovvero al mancato rispetto di standard doverosi*" attinenti all'organizzazione e all'attività dell'Ente, difetto riconducibile alla politica d'impresa oppure a deficit strutturali e prescrittivi nell'organizzazione aziendale.

In sostanza, affinché il Reato non venga imputato ad esso in maniera soggettiva, l'Ente deve dimostrare di aver fatto tutto quanto in suo potere per prevenire nell'esercizio dell'attività di impresa la commissione di uno dei Reati previsti dal Decreto (sulle condizioni di esenzione da responsabilità previste dal Decreto si veda *infra sub* paragrafo 0).

1.4 Le sanzioni applicabili all'Ente

Le sanzioni previste dal Decreto a carico dell'Ente, in conseguenza della commissione o tentata commissione dei Reati Presupposto, sono di quattro tipi:

a) Sanzione pecuniaria

È sempre applicata quando il giudice ritenga l'Ente responsabile. Viene determinata attraverso un sistema basato su "quote" (in numero non inferiore a cento e non superiore a mille), ciascuna di valore tra un minimo di Euro 258,23 ed un massimo di Euro 1.549,37. La sanzione pecuniaria, pertanto, oscilla tra un minimo di Euro 25.823 ed un massimo di Euro 1.549.370 (eccetto per i reati

societari le cui sanzioni pecuniarie sono raddoppiate in base a quanto previsto dalla Legge sul Risparmio 262/2005, art. 39, comma 5). Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente, nonché dell'eventuale attività svolta dallo stesso per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione.

La sanzione pecuniaria è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di 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;
- è stato adottato o reso operativo un Modello organizzativo idoneo a prevenire Reati della specie di quello verificatesi.

Inoltre è prevista la riduzione della metà della sanzione pecuniaria se:

- l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità.

Il principio fondamentale che guida l'intera materia della responsabilità dell'Ente, stabilisce che dell'obbligazione per il pagamento della sanzione pecuniaria inflitta all'Ente risponde soltanto l'Ente, con il suo patrimonio o il fondo comune. La norma, dunque, esclude una responsabilità patrimoniale diretta dei soci o degli associati, indipendentemente dalla natura giuridica dell'Ente collettivo.

b) Sanzioni interdittive

Si tratta dell'interdizione dall'esercizio dell'attività, della sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, del divieto di contrattare con la Pubblica Amministrazione, dell'esclusione da agevolazioni, finanziamenti, contributi, sussidi ed eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive sono irrogate, congiuntamente a quella pecuniaria, solo se espressamente previste per quella fattispecie di reato, e soltanto quando ricorre almeno una di queste due condizioni:

- l'Ente ha già commesso in precedenza un illecito da reato (reiterazione degli illeciti);
- l'Ente ha tratto dal reato un profitto di rilevante entità.

c) Confisca

Consiste nell'acquisizione da parte dello Stato del prezzo o del profitto del reato, anche in forma per equivalente (confiscando cioè una somma di denaro, beni o altre utilità di valore corrispondenti al prezzo o profitto del reato).

d) Pubblicazione della sentenza

Consiste nella pubblicazione della sentenza di condanna (per intero o per estratto e a spese dell'Ente) su uno o più giornali indicati dal giudice nonché mediante affissione nel Comune in cui l'Ente ha la propria sede principale. La pubblicazione della sentenza può essere disposta dal giudice quando nei confronti dell'Ente viene applicata una sanzione interdittiva.

Il Pubblico Ministero, infine, può chiedere l'applicazione delle sanzioni interdittive anche in via cautelare, qualora sussistano gravi indizi della responsabilità dell'Ente o vi siano fondati e specifici

elementi tali da far ritenere il concreto pericolo che vengano commessi illeciti dello stesso tipo di quello già commesso.

1.5 L'esenzione dalla responsabilità: il Modello di organizzazione, gestione e controllo ex D.lgs. 231/2001

Il Decreto, nell'introdurre il sopra descritto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero dalla stessa qualora l'Ente dimostri di aver adottato tutte le misure organizzative necessarie al fine di prevenire la commissione dei Reati previsti dal Decreto da parte di soggetti che operino per suo conto.

In particolare, l'Ente va esente da responsabilità se prova:

- che l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- che il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- che non vi è stata omessa o insufficiente vigilanza da parte del predetto organismo.

Le condizioni appena elencate devono concorrere congiuntamente affinché la responsabilità dell'Ente possa essere esclusa. L'esenzione da colpa della Società dipende quindi dall'adozione ed attuazione efficace di un Modello di prevenzione dei reati e dalla istituzione di un Organismo di Vigilanza sul Modello, a cui è assegnata la responsabilità di sorvegliare la conformità della attività agli standard e alle procedure definite nel Modello.

Nonostante il Modello funga da causa di non punibilità sia che il Reato Presupposto sia stato commesso da un soggetto in posizione apicale, sia che sia stato commesso da un soggetto in posizione subordinata, il Decreto è molto più rigido e severo nel caso in cui il reato sia stato commesso da un Soggetto Apicale, poiché, in tal caso, opera un'inversione dell'onere della prova ed è l'Ente che deve dimostrare che il reato è stato commesso dal proprio funzionario in posizione apicale eludendo fraudolentemente il Modello. Il Decreto richiede una prova di estraneità più forte in quanto l'Ente deve provare una sorta di "frode interna" da parte di Soggetti Apicali.

Nell'ipotesi di reati commessi da soggetti in posizione subordinata, invece, l'Ente può essere chiamato a rispondere solo qualora si accerti che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza sullo stesso gravanti. Si tratta, in questo caso, di una vera e propria colpa in organizzazione: la Società ha acconsentito indirettamente alla commissione del reato, non presidiando le attività e i soggetti a rischio di commissione di un Reato Presupposto.

Dotarsi di un Modello ai sensi del Decreto non è obbligatorio ai sensi di legge, anche se, in base ai criteri di imputazione del Reato all'Ente, il Modello è l'unico strumento che, se efficacemente attuato, può eventualmente evitare un coinvolgimento dell'Ente nella commissione dei Reati previsti dal Decreto. Ne consegue, pertanto, che l'adozione di un Modello efficace ed efficiente è nell'interesse della Società.

Quanto alle caratteristiche che un Modello deve possedere per essere considerato "idoneo", l'art. 6 comma 2 del Decreto precisa che il Modello deve:

- individuare le attività dell'Ente nel cui ambito esiste la possibilità che siano commessi i reati di cui al Decreto;

- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- uno o più canali che consentano di presentare segnalazioni di condotte illecite rilevanti ai sensi del Decreto;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

1.6 I reati commessi all'estero

La responsabilità prevista dal Decreto si configura anche in relazione ai Reati commessi all'estero dall'Ente, a condizione che:

- il Reato sia stato commesso da un soggetto funzionalmente legato all'Ente, sia esso Soggetto Apicale o Soggetto Subordinato;
- l'Ente abbia la propria sede principale in Italia;
- sussistano le condizioni generali di procedibilità previste dagli articoli 7, 8, 9 e 10 c.p. per poter perseguire in Italia un reato commesso all'estero (qualora la legge preveda che la persona fisica colpevole sia punita a richiesta del Ministro della Giustizia, si procede contro l'Ente solo se la richiesta è formulata anche nei confronti dell'Ente stesso);
- non proceda lo Stato del luogo in cui è stato commesso il Reato.

1.7 Le linee guida di Confindustria

Il Decreto, all'art. 6, comma 3, prevede che i Modelli di organizzazione gestione e controllo possano essere adottati dagli Enti sulla base di codici di comportamento redatti dalle associazioni di categoria e comunicati al Ministero della Giustizia.

La prima associazione di categoria a redigere un documento di indirizzo per la costruzione dei modelli è stata Confindustria che, nel marzo del 2002, ha emanato le proprie "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001" (successivamente modificate e aggiornate, dapprima nel maggio 2004, poi nel marzo 2008 e nel marzo 2014 e, da ultimo, nel giugno 2021).

Le linee guida di Confindustria dettate per le PMI hanno rappresentato un riferimento per la Società nella stesura del presente Modello Organizzativo. In particolare, esse prevedono che la costruzione dei modelli di organizzazione, gestione e controllo, debba avvenire secondo le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare nel contesto aziendale i reati previsti dal D.Lgs. 231/2001;
- la predisposizione di un sistema di controllo idoneo a prevenire i rischi di reato identificati nella fase precedente, da effettuarsi attraverso la valutazione del sistema di controllo esistente e il relativo grado di adeguamento alle esigenze di prevenzione espresse dal D.Lgs. 231/2001.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida di Confindustria per garantire l'efficacia del Modello di organizzazione, gestione e controllo sono di seguito riassunte:

- la previsione di principi etici e di regole comportamentali in un Codice di Condotta;
- un sistema organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e alla descrizione dei compiti;
- procedure manuali e/o informatiche che regolino lo svolgimento delle attività, prevedendo gli opportuni e adeguati controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, laddove opportuno, limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

2. LA SOCIETÀ

2.1 Attività e struttura organizzativa di Security Lab

Security Lab, attiva dal 2011, è una Società a responsabilità limitata avente sede legale in Milano (MI), Largo Francesco Richini 2/A, 20122 e presenta una sede secondaria in Via Trento 90, Meda (MB), 20821.

Security Lab ha come oggetto sociale lo sviluppo e la commercializzazione di soluzioni in ambito "*Network & Cybersecurity*", ossia di apparecchiature e loro componenti destinate alla protezione, alla sicurezza e alla gestione delle infrastrutture di rete (quali, a titolo esemplificativo, firewall, antispam, single sign on, ecc.).

2.2 Sistema di Governance di Security Lab

La Società ha adottato il seguente modello di *governance*:

- l'Assemblea Soci è competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o dallo statuto. Le deliberazioni dell'assemblea sono constatate dal processo verbale firmato dal presidente e segretario.
- Il Consiglio di Amministrazione, costituito da tre componenti, è investito dei più ampi poteri per il conseguimento degli scopi sociali e per la gestione ordinaria e straordinaria della Società, fatta eccezione soltanto per quegli atti che, a norma di legge e dello statuto, sono di esclusiva competenza dell'Assemblea.

3. ADOZIONE DEL MODELLO DA PARTE DI SECURITY LAB

3.1 Sistema di deleghe e autorizzazioni

Come chiarito dalle linee guida di Confindustria, i poteri autorizzativi e di firma devono essere assegnati in coerenza alle responsabilità organizzative e gestionali definite, prevedendo, quando

richiesto, una puntuale indicazione delle soglie di approvazione delle spese, specialmente nelle aree considerate “a rischio reato”.

Il Consiglio di Amministrazione di Security Lab S.r.l. è l’organo dotato dei poteri di firma e preposto a conferire ed approvare formalmente, ove necessario, le deleghe ed i poteri autorizzativi.

3.2 Finalità del Modello

Con l’adozione del presente Modello di organizzazione, gestione e controllo ai sensi dell’art. 6 del Decreto, Security Lab intende adempiere alle prescrizioni del Decreto per migliorare e rendere quanto più efficiente possibile il proprio sistema di controllo interno.

Obiettivo principale del Modello, infatti, è quello di creare un sistema organico e strutturato di principi comportamentali e procedure di controllo, atto a prevenire, ove possibile e concretamente fattibile, la commissione dei reati previsti dal Decreto. Il Modello rappresenta una componente fondamentale del sistema di governo della Società e costituisce l’estrinsecazione di una cultura di gestione improntata alla correttezza, alla trasparenza e alla legalità che Security Lab intende promuovere e diffondere a tutto il suo personale.

Il Modello si propone, pertanto, le seguenti finalità:

- vietare comportamenti che possano integrare le fattispecie illecite previste dal Decreto;
- fornire un’adeguata informazione a coloro che agiscono su mandato della Società, o sono legati alla stessa da rapporti rilevanti ai fini del Decreto, sulle attività che comportano il rischio di commissione di reati;
- diffondere la consapevolezza in tutti coloro che operano in nome e per conto della Società di poter incorrere, in caso di violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice di Condotta, in un illecito passibile di sanzioni, non solo nei propri confronti ma anche nei confronti dell'azienda;
- diffondere una cultura di gestione che sia improntata alla legalità, in quanto la Società condanna ogni comportamento non conforme alla legge o alle disposizioni interne, e in particolare alle disposizioni contenute nel proprio Modello e nel proprio Codice di Condotta;
- diffondere una cultura del controllo e di *risk management*;
- attuare un’efficace ed efficiente organizzazione dell’attività, ponendo l’accento sulla formazione delle decisioni e sulla loro trasparenza e tracciabilità documentale, sulla responsabilizzazione delle risorse dedicate all’assunzione di tali decisioni e della relativa attuazione, sulla previsione di controlli, preventivi e successivi, nonché sulla corretta gestione dell’informazione interna ed esterna;
- attuare tutte le misure necessarie per ridurre il più possibile il rischio di commissione di reati, valorizzando i presidi in essere atti a scongiurare condotte illecite rilevanti ai sensi del Decreto.

3.3 Metodologia di predisposizione del Modello della Società

Il Modello di Security Lab, ispirato alle Linee Guida di Confindustria, è stato elaborato tenendo conto dell’attività concretamente svolta dalla Società, della sua struttura, della natura e delle dimensioni della sua organizzazione.

Resta inteso che il Modello verrà sottoposto agli aggiornamenti che si renderanno necessari, in base alla futura evoluzione della normativa, della struttura organizzativa della Società e del contesto in cui la stessa si troverà ad operare.

Security Lab ha proceduto ad un'analisi preliminare del proprio contesto e, successivamente, ad un'analisi delle aree di attività che presentano profili potenziali di rischio, in relazione alla commissione dei Reati Presupposto indicati dal Decreto. In particolar modo, sono stati analizzati: la storia della Società, il contesto societario, il settore di appartenenza, l'assetto organizzativo, il sistema di *governance* esistente, i principali rapporti giuridici esistenti con soggetti terzi, la realtà operativa, le prassi e le procedure formalizzate e diffuse all'interno della Società a presidio delle Attività Sensibili.

Ai fini della preparazione del presente documento, coerentemente con le disposizioni del Decreto, con le Linee Guida di Confindustria e con le indicazioni desumibili ad oggi dalla giurisprudenza, la Società ha proceduto dunque:

- all'identificazione, mediante interviste al *management*, dei processi o attività in cui è possibile che siano commessi i Reati Presupposto indicati nel Decreto;
- all'autovalutazione dei rischi (c.d. *risk self-assessment*) di commissione di Reati e del sistema di controllo interno idoneo a prevenire comportamenti illeciti;
- all'identificazione dei presidi di controllo - già esistenti o da implementare nelle procedure operative e prassi aziendali - necessari per la prevenzione o per la mitigazione del rischio di commissione dei Reati Presupposto;
- all'analisi del proprio sistema di poteri e di attribuzione delle responsabilità.

3.4 Struttura del Modello: parte generale e parte speciale

Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale".

La Parte Generale, partendo da un sommario esame del contenuto del Decreto, si propone di definire la struttura del Modello, disciplinandone finalità e destinatari, individuando funzione e composizione dell'OdV, istituendo un sistema di flussi informativi e un sistema disciplinare idoneo a sanzionare il mancato rispetto del Modello stesso.

La Parte Speciale, invece, è predisposta per le diverse tipologie di reato contemplate nel Decreto e ritenute, all'esito dell'attività di *self-risk assessment*, astrattamente ipotizzabili in capo alla Società. Essa si propone di disciplinare concretamente le condotte dei soggetti aziendali, apicali e sottoposti all'altrui direzione e vigilanza, al fine di prevenire la commissione delle fattispecie criminose potenzialmente rilevanti per la Società, mediante l'elaborazione di distinte regole di condotta, protocolli e procedure, operanti all'interno delle differenti aree a rischio.

Si rileva, inoltre, che l'introduzione di alcuni reati nel presente Modello ha carattere meramente prudenziale in quanto, pur non sussistendo elementi specifici da cui dedurre l'esistenza di attuali rischi, si tratta di reati sui quali la Società intende comunque mantenere un alto livello di attenzione.

La Parte Speciale si compone di diverse sezioni relative alle categorie di reato astrattamente applicabili alla Società e raggruppate come segue:

Parte Speciale	Categoria di reati rilevanti
A	Reati contro la Pubblica Amministrazione
B	Reati societari

C	Corruzione tra privati
D	Delitti informativi e violazione del diritto d'autore
E	Reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro 25
F	Delitti di criminalità organizzata – Reati transnazionali - Delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria 36
G	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio
H	Reati tributari

3.5 I Destinatari del Modello

Le disposizioni del Modello sono vincolanti per:

- il Consiglio di Amministrazione e tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione, controllo, nonché funzioni di carattere disciplinare, consultivo e propositivo all'interno della Società o in una sua unità organizzativa autonoma, inclusi i membri degli organi della associazione;
- i dipendenti della Società, per tali intendendosi tutti coloro che sono legati a Security Lab da un rapporto di lavoro subordinato, anche se distaccati per lo svolgimento della loro attività;
- tutti quei soggetti che collaborano con Security Lab in forza di un rapporto di lavoro parasubordinato e per i collaboratori sottoposti alla direzione o vigilanza del *management* della Società;
- coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa (quali legali, consulenti, agenti, distributori ecc.);
- tutti quei soggetti che agiscono nell'interesse della Società in quanto legati alla stessa da rapporti giuridici contrattuali o da accordi di altra natura, quali, ad esempio, partner o terze parti per la realizzazione o l'acquisizione di un progetto (di seguito, collettivamente, i "Destinatari").

Eventuali dubbi sull'applicabilità o sulle modalità di applicazione del Modello ad un soggetto o ad una classe di soggetti terzi, possono essere risolti dall'Organismo di Vigilanza interpellato dal responsabile dell'area/funzione interessata.

3.6 Approvazione, modifiche e aggiornamento del Modello

Il Modello, in conformità alle prescrizioni dell'art. 6, comma I lett. a) del Decreto, è un "*atto di emanazione dell'organo dirigente*". Per questa ragione è demandato all'Organo amministrativo (nel caso di specie, il Consiglio di Amministrazione di Security Lab) di provvedere, mediante apposita delibera, all'adozione del Modello ai sensi del Decreto, in funzione dei profili di rischio configurabili nelle attività svolte dalla Associazione.

L'Organo di gestione, inoltre, è responsabile dell'aggiornamento del Modello e del suo adeguamento, anche in conseguenza di eventuali mutamenti degli assetti organizzativi o dei processi operativi, di significative violazioni del Modello stesso o di modifiche legislative.

A tal fine, è attribuito all'Organismo di Vigilanza (di seguito anche "**OdV**") il compito di formulare al vertice aziendale proposte di aggiornamento e adeguamento del Modello e delle procedure o dei protocolli – che ne costituiscono parte integrante.

È rimessa, invece, alla responsabilità della Società l'applicazione del Modello in relazione all'attività dalla stessa in concreto posta in essere.

Per le modifiche e gli aggiornamenti al Modello, la Società si avvale di tutte le funzioni aziendali e, ove ritenuto necessario, di consulenti esterni.

4. L'ORGANISMO DI VIGILANZA

4.1 Identificazione dell'Organismo di Vigilanza. Composizione, nomina, revoca, cause di ineleggibilità e decadenza

L'art. 6 del Decreto prevede che l'Ente possa essere esonerato dalla responsabilità conseguente alla commissione dei reati presupposto se l'organo amministrativo ha, fra l'altro, "*affidato il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo*".

L'affidamento di detti compiti all'OdV e, ovviamente, il corretto ed efficace svolgimento degli stessi, sono presupposti indispensabili per l'esonero dell'Ente dalla responsabilità, sia che il reato sia stato commesso dai Soggetti Apicali, sia che sia stato commesso dai Soggetti Sottoposti.

In attuazione di quanto previsto dal Decreto, la Società ha istituito un Organismo di Vigilanza monocratico composto da un membro. L'Organismo di Vigilanza resta in carica tre anni ed è in ogni caso rieleggibile. La composizione dell'OdV assicura il rispetto dei seguenti requisiti:

- ***Autonomia***: l'OdV deve avere autonomia decisionale, qualificabile come imprescindibile libertà di autodeterminazione e d'azione, con totale esercizio della discrezionalità tecnica nell'espletamento delle proprie funzioni;
- ***indipendenza rispetto alla Società***: l'OdV deve essere scevro da condizionamenti dipendenti da legami di sudditanza rispetto al vertice di controllo e deve essere organo terzo, collocato in posizione di indipendenza anche gerarchica, capace di adottare provvedimenti ed iniziative autonome;
- ***professionalità***: l'OdV deve essere professionalmente capace ed affidabile, sia per quanto riguarda i singoli membri che lo compongono, sia nella sua globalità. Deve disporre, come organo, delle cognizioni tecniche e delle professionalità necessarie al fine di espletare al meglio le funzioni affidategli;
- ***continuità d'azione***: l'OdV deve svolgere le funzioni assegnategli in via continuativa, seppure non in modo esclusivo;
- ***onorabilità ed assenza di conflitti di interesse***: non può essere nominato membro dell'OdV e, se del caso, decade dalla carica, il soggetto che sia interdetto, inabilitato o fallito o che sia comunque stato condannato per uno dei reati previsti dal Decreto o,

comunque, ad una delle pene che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi.

Il Consiglio di Amministrazione di Security Lab provvede, mediante delibera, alla nomina ed alla revoca dei membri dell'OdV.

Costituiscono cause di ineleggibilità o decadenza da membri dell'Organismo di Vigilanza:

- la condizione di essere stati sottoposti a misure di prevenzione disposte dall'Autorità Giudiziaria ai sensi della legge 27 dicembre 1956 n. 1423 (legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità) o della legge 31 maggio 1965 n. 575 (disposizioni contro la mafia);

- la condizione di essere indagati o di essere stati condannati, anche con sentenza non ancora definitiva o emessa ex artt. 444 e ss. c.p.p. (patteggiamento) o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione (i) per uno o più illeciti tra quelli tassativamente previsti dal Decreto, ovvero (ii) alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo.

- la condizione di essere interdetto, inabilitato, fallito o essere stato condannato, anche con sentenza non definitiva, ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi.

Il verificarsi anche di una sola delle suddette condizioni comporta l'ineleggibilità alla carica di membro dell'OdV e, in caso di elezione, la decadenza automatica da detta carica, senza necessità di una determina da parte del Consiglio di Amministrazione, che provvederà alla sostituzione.

I componenti dell'OdV cessano il proprio ruolo per rinuncia, sopravvenuta incapacità, morte o revoca. L'eventuale termine del rapporto lavorativo tra il componente dell'Organismo di Vigilanza e la Società comporta automaticamente la revoca dall'incarico.

I componenti dell'OdV possono essere revocati dal Consiglio di Amministrazione per giusta causa. A titolo esemplificativo e non esaustivo, costituiscono giusta causa di revoca:

- l'accertamento di un grave inadempimento da parte dell'Organismo di Vigilanza nello svolgimento dei propri compiti;

- l'omessa comunicazione di un conflitto di interessi che impedisca il mantenimento del ruolo di componente dell'Organismo stesso;

- la sopravvenienza di cause di ineleggibilità o decadenza;

- la violazione degli obblighi di riservatezza in ordine alle notizie e alle informazioni acquisite nell'esercizio delle funzioni proprie dell'Organismo di Vigilanza;

- per i componenti legati alla Società da un rapporto di lavoro subordinato, l'avvio di un procedimento disciplinare per fatti da cui possa derivare la sanzione del licenziamento.

In caso di rinuncia, sopravvenuta incapacità, morte o revoca di un componente dell'Organismo di Vigilanza, il Presidente dell'OdV ne darà comunicazione tempestiva al Consiglio di Amministrazione, il quale prenderà le decisioni del caso.

In caso di rinuncia, sopravvenuta incapacità, morte o revoca del Presidente dell'OdV, subentra a questi il membro più anziano, il quale rimane in carica fino alla data in cui il Consiglio di Amministrazione abbia deliberato la nomina del nuovo Presidente dell'Organismo medesimo.

Fermo restando quanto sopra, la disciplina del funzionamento dell'Organismo di Vigilanza è rimessa all'Organismo stesso che, una volta nominato, è chiamato ad adottare un proprio Regolamento interno.

4.2 Funzioni e Poteri

Ferma restando la responsabilità del Consiglio di Amministrazione in merito all'adozione, implementazione e aggiornamento del Modello, all'Organismo di Vigilanza della Società è affidato il compito di vigilare:

- sull'osservanza delle prescrizioni del Modello da parte dei Destinatari;
- sulla reale efficacia ed effettiva capacità del Modello di prevenire la commissione dei Reati Presupposto;
- sull'adeguatezza del Modello, segnalando l'opportunità di aggiornamento dello stesso laddove riscontri esigenze di adeguamento in relazione a mutate condizioni aziendali e/o all'introduzione di modifiche nella normativa di riferimento.

Sul piano operativo è affidato all'OdV il compito di:

- attivare le necessarie procedure di controllo, tenendo presente che la responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata al *management* operativo della Società e forma parte integrante del processo aziendale, il che conferma l'importanza di un processo formativo del personale;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle attività a rischio come definite nelle singole Parti Speciali del Modello;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV, o tenute a sua disposizione;
- effettuare incontri periodici con le funzioni responsabili dei processi a rischio per il migliore monitoraggio delle attività nelle aree a rischio reato. A tal fine, l'OdV viene tenuto costantemente informato sull'evoluzione delle attività nelle suddette aree a rischio e ha libero accesso a tutta la documentazione aziendale rilevante. All'OdV devono essere inoltre segnalate da parte del management eventuali situazioni dell'attività aziendale che possono esporre l'azienda al rischio di commissione di un reato;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e per la predisposizione della documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità ed effettuando tutti gli accertamenti ritenuti necessari od opportuni;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello delle quali sia venuto a conoscenza;
- comunicare eventuali violazioni del Modello agli organi competenti della Società in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;

- coordinarsi con i responsabili delle altre funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello;
- mantenere un collegamento costante con gli organi di controllo della Società e con gli altri consulenti coinvolti nelle attività di attuazione del Modello.

Le attività poste in essere dall'OdV non possono essere sindacate da alcun organismo o struttura aziendale, fermo restando che il Consiglio di Amministrazione vigilerà sull'adeguatezza del suo intervento, poiché ad egli compete la responsabilità ultima del funzionamento e dell'efficacia del Modello ed il potere di adottarlo e di darvi attuazione.

L'OdV, come sopra indicato, deve avere libero accesso a tutta la documentazione in possesso della Società – senza necessità di alcun consenso preventivo – onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei propri compiti.

I componenti dell'OdV sono tenuti al segreto in ordine alle notizie ed alle informazioni acquisite nell'esercizio delle loro funzioni e devono astenersi dal ricercare e dall'utilizzare le suddette informazioni per motivi diversi dall'espletamento del loro incarico.

L'OdV della Società è dotato di appropriata autonomia di spesa, attraverso la previsione di un budget annuale da utilizzare per lo svolgimento delle proprie attività e il ricorso a consulenti esterni nei casi in cui ciò si renda necessario. Le eventuali spese straordinarie saranno sottoposte all'approvazione del Consiglio di Amministrazione.

4.3 Attività di reporting

L'Organismo di Vigilanza si relaziona costantemente con gli organi della Società e, in particolare, con il Consiglio di Amministrazione.

A tal fine, l'Organismo di Vigilanza riferirà al Consiglio di Amministrazione:

- all'occorrenza, in merito alla formulazione delle proposte per gli eventuali aggiornamenti ed adeguamenti del Modello;
- immediatamente, in merito alle violazioni accertate del Modello, nei casi in cui tali violazioni possano comportare l'insorgere di una responsabilità in capo alla Società, affinché vengano presi opportuni provvedimenti;
- periodicamente, con una relazione informativa, su base annuale, avente ad oggetto:
    - le attività di verifica e controllo compiute e l'esito delle stesse;
    - una sintesi delle segnalazioni ricevute e delle azioni eventualmente intraprese a seguito delle stesse;
    - eventuali criticità emerse in termini di comportamenti o eventi che possono avere un effetto sull'adeguatezza o sull'efficacia del Modello e gli opportuni interventi correttivi o migliorativi;
    - l'individuazione del piano di lavoro per l'anno successivo.

L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione e potrà, a sua volta, presentare richiesta in tal senso, per riferire in merito al funzionamento del Modello o a situazioni specifiche.

4.3.1 Flussi informativi all'Organismo di Vigilanza

Il D.Lgs. 231/2001 enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di specifici obblighi informativi nei confronti dell'Organismo di Vigilanza (c.d. **Flussi informativi**) da parte delle Funzioni aziendali, diretti a consentire all'Organismo stesso lo svolgimento delle proprie attività di vigilanza e di verifica.

A tal fine, dovranno essere trasmessi all'OdV i seguenti flussi informativi:

- su base periodica, informazioni, dati, notizie e documenti costituenti deroghe e/o eccezioni rispetto alle procedure aziendali o attinenti alla gestione dei processi aziendali a rischio-reato identificati dall'Organismo e formalmente richiesti alle singole Funzioni ("*Flussi informativi periodici*");
- fatti, notizie, documenti, dati e informazioni relativi al verificarsi di determinati eventi ("*Flussi informativi ad evento*"), quali, a titolo esemplificativo e non esaustivo:
    - notizie relative alla commissione o alla ragionevole convinzione di commissione degli illeciti previsti dal Decreto;
    - violazioni delle regole di comportamento o procedurali contenute nel presente Modello e nel Codice di Condotta;
    - richieste di assistenza legale inoltrate dai dipendenti nei confronti dei quali la magistratura procede per i reati previsti dal Decreto;
    - provvedimenti e notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra Autorità dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, qualora tali indagini coinvolgano la Società, i suoi dipendenti, i membri degli organi della Società o altri Destinatari/collaboratori esterni;
    - notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza di eventuali procedimenti disciplinari svolti e delle eventuali sanzioni irrogate;
    - accessi, ispezioni, notifiche e richieste delle Autorità o delle Forze dell'Ordine;
    - infortuni sul lavoro;
    - modifiche del sistema di deleghe e procure in vigore e degli organigrammi aziendali.

Si precisa che l'OdV potrà raccogliere direttamente le informazioni di cui sopra nell'espletamento delle proprie attività di controllo, attraverso le modalità che lo stesso riterrà più opportune (ad es. attraverso la conduzione di interviste ai Responsabili di funzione, la predisposizione di questionari e reportistica *ad hoc*, attività di audit, ecc.).

Per una disamina dei flussi informativi di dettaglio si rimanda al contenuto della procedura "*Sistema di reporting all'Organismo di Vigilanza*".

4.3.2. La legge n. 179/2017 e il c.d. "Whistleblowing"

La Legge n. 179/2017, entrata in vigore il 29 dicembre 2017, oltre a modificare la disciplina del *whistleblowing* per il settore pubblico, ha apportato alcune modifiche al D. Lgs. 231/2001 aggiungendo tre nuovi commi all'art. 6 ed introducendo delle disposizioni per la tutela del dipendente che segnali illeciti nel settore privato.

In particolare, a seguito della novella legislativa, i Modelli Organizzativi devono prevedere:

- uno o più canali che consentono ai soggetti apicali o sottoposti all'altrui direzione e vigilanza, di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del Modello Organizzativo di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

- almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente alla segnalazione;

- nel sistema disciplinare, sanzioni nei confronti di chi violi le misure a tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelino infondate.

In attuazione di quanto sopra, Security Lab ha implementato canali di comunicazione ad hoc per la trasmissione delle segnalazioni di condotte potenzialmente illecite ovvero di violazioni alle disposizioni del Decreto o del proprio Modello e/o del Codice di Condotta (c.d. "incidenti di *compliance"*) e pone il divieto di ogni forma di ritorsione o discriminazione, diretta o indiretta, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione .

Nello specifico, la Società ha istituito i seguenti canali dedicati:

- un indirizzo di posta ordinaria, coincidente con la sede legale della stessa in Largo Francesco Richini 2/A, Milano (MI), 20122;

- un indirizzo di posta elettronica odv@security-lab.it reso noto al personale aziendale e con accesso riservato ai soli componenti dell'Organismo di Vigilanza.

L'Organismo di Vigilanza monitorerà sistematicamente tali canali e, laddove riscontrasse la presenza di segnalazioni potenzialmente rilevanti ai sensi del Decreto, dopo averne accertata la fondatezza, ne darà tempestiva informativa al Consiglio di Amministrazione.

In ogni caso, l'Organismo di Vigilanza si impegna a tutelare la riservatezza dell'identità del segnalante nelle fasi di gestione della segnalazione e nel corso delle eventuali indagini interne.

A seconda della gravità dell'incidente di *compliance* e delle implicazioni conseguenti, Security Lab applica misure correttive adeguate, incluse eventuali sanzioni disciplinari.

5. SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DEL MODELLO

5.1 Principi generali

Security Lab condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del proprio Modello e Codice di Condotta, anche qualora il comportamento stesso sia realizzato nell'interesse della Società ovvero con l'intenzione di arrecare ad essa un vantaggio.

La Società, infatti, ritiene che le violazioni dei principi comportamentali e delle procedure previste dal Modello e dal Codice di Condotta ledano il rapporto di fiducia instaurato con l'ente e, di conseguenza, tali condotte comportano l'applicazione di azioni disciplinari, anche a prescindere

dall'istaurazione di un eventuale giudizio penale nel caso in cui il predetto comportamento costituisca reato.

Inoltre, la predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello e nel Codice di Condotta è condizione essenziale per assicurare l'effettività del Modello stesso e per rendere efficace l'azione di vigilanza dell'OdV.

Al riguardo, infatti, l'art. 6 comma 2, lettera e) del Decreto prevede che i Modelli di Organizzazione, Gestione e Controllo debbano "*introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello*".

Il sistema disciplinare, così come previsto dall'art. 7, comma 1, Legge 300/1970 (Statuto dei lavoratori), sarà affisso nella bacheca aziendale.

L'accertamento delle infrazioni può essere avviato anche su iniziativa dell'OdV qualora, nel corso della propria attività di controllo e vigilanza, abbia rilevato una possibile violazione del Modello.

L'irrogazione delle sanzioni nei confronti dei dipendenti è di competenza del *management* aziendale, in linea con l'assetto di poteri definito.

L'accertamento delle eventuali responsabilità derivanti dalla violazione del Modello e l'attribuzione della conseguente sanzione devono essere comunque condotti nel rispetto della vigente normativa, della tutela della privacy, della dignità e della reputazione dei soggetti coinvolti.

In generale, le violazioni possono essere ricondotte ai seguenti comportamenti e classificate come segue:

- comportamenti che integrano una mancata attuazione colposa delle prescrizioni del Modello, ivi comprese direttive, procedure o istruzioni aziendali, incluse specifiche indicazioni regolamentari e procedure in materia di sicurezza sul lavoro;
- comportamenti che integrano una grave trasgressione dolosa delle prescrizioni del Modello ivi comprese specifiche indicazioni regolamentari e procedure in materia di sicurezza sul lavoro, tali da compromettere il rapporto di fiducia tra l'autore del fatto e la Società, in quanto preordinate univocamente a commettere un reato.

Le sanzioni disciplinari previste dal presente Modello si applicano anche ai casi di violazione delle misure poste a tutela del segnalante, nonché a coloro i quali dovessero effettuare segnalazioni infondate con dolo o colpa grave.

5.2 Sanzioni per i lavoratori dipendenti

L'effettiva operatività del presente Modello è garantita da un adeguato Sistema disciplinare che sanziona il mancato rispetto e la violazione delle norme contenute nel Modello stesso e dei suoi elementi costitutivi. Simili violazioni devono essere sanzionate in via disciplinare, a prescindere dall'eventuale instaurazione di un giudizio penale, in quanto ledono il rapporto di fiducia con la Società, in qualità di datore di lavoro, e configurano una violazione degli obblighi di diligenza e fedeltà del lavoratore di cui agli artt. 2104 e 2105 c.c.

La violazione da parte dei dipendenti delle singole regole comportamentali di cui al presente Modello costituisce, pertanto, illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori, nel rispetto dell'art. 7 della legge 30 maggio 1970, n. 300 (Statuto dei lavoratori), sono quelli previsti dal CCNL applicato (CCNL del commercio e terziario). In particolare:

- incorre nel provvedimento del **richiamo verbale** il lavoratore che:
    - in forma lieve violi le procedure interne previste dal presente Modello o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso;
- incorre nel provvedimento dell'**ammonizione scritta** il lavoratore che:
    - risulti recidivo rispetto alle infrazioni di cui al punto che precede;
- incorre nel provvedimento della **multa non superiore a 3 ore di retribuzione** il lavoratore che:
    - oltre la terza volta nell'anno solare, violi le procedure interne previste dal presente Modello o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso o del Codice di Condotta;
- incorre nel provvedimento della **sospensione dal lavoro e dalla retribuzione per un periodo fino a tre giorni** il lavoratore che:
    - commetta violazioni gravi di una o più regole procedurali o comportamentali previste nel presente Modello o dal Codice di Condotta quando, da tale violazione, non derivi pregiudizio alla normale attività della Società;
    - per il livello di responsabilità gerarchico o tecnico, o in presenza di circostanze aggravanti, leda l'efficacia del Modello con comportamenti quali:
        - l'inosservanza dell'obbligo di informativa all'Organismo di Vigilanza;
        - l'inosservanza del divieto di applicare misure ritorsive o discriminatorie a carico di un whistleblower in ragione della segnalazione;
- incorre nel provvedimento del **licenziamento senza preavviso** il lavoratore che:
    - nel violare le procedure interne previste dal presente Modello o adottando, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, nonché compiendo atti contrari all'interesse della Società, la esponga ad una situazione di pericolo per l'integrità dei suoi beni, anche in assenza di danno o, nei casi più gravi, determini la concreta applicazione a carico di Security Lab di alcuna delle misure previste dal Decreto.

5.3 Misure nei confronti dei dirigenti

Tenuto conto della particolare connotazione della figura del dirigente ad opera della specifica disciplina normativa e contrattuale, in caso di grave violazione di una o più prescrizioni del Modello o del Codice di Condotta tale da configurare un notevole inadempimento, ovvero in caso di violazioni tali da ledere irreparabilmente il rapporto di fiducia instaurato con la Società, il Consiglio di Amministrazione di Security Lab adotterà i provvedimenti che riterrà in concreto più opportuni, in linea con quanto previsto dal CCNL Dirigenti Industria, dandone tempestiva comunicazione all'Organismo di Vigilanza.

5.4 Misure nei confronti dell'organo amministrativo

Anche il Consiglio di Amministrazione è passibile delle sanzioni previste nel presente Sistema Disciplinare per l'ipotesi di violazione delle previsioni del Modello.

Qualora sia accertata una violazione del Modello o del Codice di Condotta di Security Lab, delle disposizioni del Decreto ovvero la realizzazione di altra condotta illecita da parte dei componenti dell'organo amministrativo, questi saranno destinatari delle seguenti misure disciplinari, che verranno applicate nel rispetto del principio di proporzionalità della sanzione al fatto commesso:

- ammonizione scritta;
- diffida al puntuale rispetto delle previsioni del Modello;
- decurtazione degli emolumenti o del corrispettivo previsto fino al 50%;
- revoca dell'incarico.

5.5 Misure nei confronti di collaboratori esterni e consulenti

Ogni comportamento posto in essere dai collaboratori esterni (consulenti, fornitori, ecc.) in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal Decreto potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali ("**clausole 231**") inserite nelle lettere di incarico, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti a Security Lab, come nel caso di applicazione delle sanzioni previste dal Decreto.

La tipologia e l'entità di ciascuna sanzione sarà definita in relazione:

- alla intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- al comportamento complessivo del collaboratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- alle modalità di conseguimento del risultato;
- alle altre particolari circostanze che accompagnano la violazione del contratto e/o del Codice di Condotta.

6. DIFFUSIONE DEL MODELLO E FORMAZIONE

6.1 Diffusione del contenuto del Modello

In linea con quanto disposto dal Decreto e dalle Linee Guida, la Società darà piena pubblicità al Modello e al Codice di Condotta, al fine di assicurare che i destinatari siano a conoscenza di tutti i loro elementi. In particolare, entrambi i documenti saranno pubblicati sulla intranet aziendale una volta formalmente approvati dal Consiglio di Amministrazione. Di tale pubblicazione verrà data notizia tramite e-mail a tutti i dipendenti della Società ai quali è fatto obbligo di rispettarne il contenuto. Lo stesso vale per ogni dipendente neo-assunto.

La comunicazione del Modello e del Codice di Condotta dovrà essere capillare, efficace, chiara e dettagliata, con aggiornamenti periodici connessi alla revisione e/o aggiornamento degli stessi.

Saranno di volta in volta definite le modalità di diffusione del Modello e del Codice di Condotta nei confronti degli ulteriori soggetti tenuti al rispetto dei contenuti degli stessi (fornitori, collaboratori esterni, consulenti e terzi in generale). In ogni caso, il Codice di Condotta e la Parte Generale del Modello, nella versione aggiornata, sono pubblicati sul sito web aziendale.

6.2 Formazione del personale

Security Lab, consapevole dell'importanza che gli aspetti formativi assumono in una prospettiva di prevenzione, organizza iniziative di formazione in materia di *compliance* obbligatorie per tutti i dipendenti.

Con l'implementazione del Modello, Security Lab si impegna a definire, in coordinamento con l'Organismo di Vigilanza, un programma di comunicazione e formazione volto a garantire la divulgazione a tutto il personale dei principali contenuti nel D. Lgs. 231/2001 e degli obblighi dallo stesso derivanti, nonché delle prescrizioni contenute nel presente Modello e nel Codice di Condotta.

Le attività di informazione e formazione nei confronti del personale saranno organizzate in presenza o in modalità *e-learning*, prevedendo diversi livelli di approfondimento in ragione del differente grado di coinvolgimento del personale nelle attività a rischio-reato. In particolare, l'attività di formazione finalizzata a diffondere la conoscenza del Decreto e le prescrizioni del Modello (c.d. "**formazione generale**") è differenziata, nei contenuti e nelle modalità di divulgazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui gli stessi operano e del fatto che gli stessi rivestano o meno funzioni di rappresentanza e gestione della Società.

L'attività di formazione generale coinvolge tutto il personale in forza, nonché tutte le risorse che in futuro saranno inserite nell'organizzazione aziendale. Le relative attività formative dovranno essere previste e concretamente effettuate sia al momento dell'assunzione, sia in occasione di eventuali mutamenti di mansioni, nonché a seguito di aggiornamenti e/o modifiche del Modello.

Security Lab continuerà, inoltre, a svolgere attività di formazione *ad hoc* nei confronti di tutti quei soggetti che, in ragione della mansione e/o dell'attività svolta, necessitano di specifiche competenze al fine di gestire i rischi peculiari all'attività stessa (c.d. "**formazione specifica**") come, a titolo esemplificativo, la formazione in materia ambientale o di salute e sicurezza nei luoghi di lavoro.

6.3 Informativa ai collaboratori esterni e ai partner commerciali

Security Lab promuove la conoscenza dei principi e delle regole di condotta previste dal Codice di Condotta e dal presente Modello anche tra i consulenti, i partner, i collaboratori a vario titolo, i clienti e i fornitori. A tali soggetti verranno, pertanto, fornite apposite informative sulle politiche e le procedure adottate dalla Società sulla base del presente Modello. I contratti che la Società sottoscriverà con i terzi conterranno specifiche clausole contrattuali (c.d. "**clausole 231**") relative al rispetto degli obblighi e dei principi derivanti dal Modello e dal Codice di Condotta, a pena di risoluzione del rapporto.