STACK EMEA – Italy S.p.A.

Modello di Organizzazione,
Gestione e Controllo
D.Lgs. 8 giugno 2001 n. 231

Versione	**Data**	**Responsabile**	**Firma**
1.0	01-07-2017	Amministratore Unico	
2.0	**31-01-2021**	CEO	
3.0	**01-03-2022**	CEO	

Sommario

1. Il Decreto Legislativo 8 Giugno 2001, n.231

Con il decreto legislativo 8 giugno 2001, n.231 è stata introdotta nell'ordinamento giuridico italiano la «*Responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*» a seguito della commissione di illecito.

I reati per i quali il decreto risulta applicabile sono:

- art. 24: «*indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche, frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture*», che correla la responsabilità amministrativa dell'ente alla commissione di reati quali l'indebita percezione di erogazioni a danno dello Stato (o di altro ente pubblico, o dell'Unione Europea), la truffa (a danno dello Stato, di un altro ente pubblico o dell'Unione Europea), la frode informatica (se commessa in danno dello Stato, di altro ente pubblico o dell'Unione europea), la frode nelle pubbliche forniture e l'indebito conseguimento di corrispettivi a carico del Fondo europeo agricolo di garanzia o per lo sviluppo rurale (art.2 legge n.898/1986);
- art. 24-bis: «*delitti informatici e trattamento illecito di dati*», che correla la responsabilità amministrativa dell'ente alla commissione di reati quali il reato di accesso abusivo ad un sistema informatico o telematico, il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, il reati di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, il reato di falsificazioni informatiche, il reato di danneggiamento di informazioni, dati e programmi informatici, ancorché, utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità ed il delitto di cui all'art.1 comma 11 D.L. 105/2019;
- art. 24-ter: «*delitti di criminalità organizzata*» che correla la responsabilità in particolare alle ipotesi di agevolazione mafiosa;

- art. 25: «*Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio*», che correla la responsabilità amministrativa dell'ente alla commissione di reati quali la concussione, l'induzione indebita a dare o promettere utilità e la corruzione per un atto d'ufficio o per un atto contrario ai doveri d'ufficio, il traffico di influenze illecite, nonché il peculato, il peculato mediante profitto dell'errore altri e abuso d'ufficio nella peculiare ipotesi in cui il fatto "offende gli interessi finanziari dell'Unione europea" -
- art. 25-bis: «*falsità in monete, in carte di pubblico credito e in valori in bollo ed in strumenti o segni di riconoscimento*» che correla la responsabilità amministrativa dell'ente alla commissione dei reati di falso nummario, di uso di valori contraffatti, di contraffazione e uso di segni distintivi e brevetti nonché l'introduzione ed il commercio di prodotti con segni falsi;
- art. 25-bis 1: «*delitti contro l'industria ed il commercio*» in particolare riferibili agli illeciti commessi nelle frodi in commercio;
- art. 25-ter: «*reati societari*», che correlano la responsabilità amministrativa dell'ente alla commissione di illeciti quali le false comunicazioni sociali, la falsità delle relazioni o nelle comunicazioni delle società di revisione, l'aggiotaggio, la illegale ripartizione degli utili e delle riserve, le illecite operazioni sulle azioni o quote sociali o della società controllante, le operazioni in pregiudizio dei creditori, l'illecita influenza sull'assemblea, l'omessa comunicazione del conflitto d'interessi, l'ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza. A questi si aggiunge la corruzione tra privati;
- art. 25 quater: «*delitti con finalità di terrorismo o di eversione dell'ordine democratico*», che correlano la responsabilità amministrativa dell'ente alla commissione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti sia nel codice penale che nelle leggi speciali;
- art. 25-quater-1: «*pratiche di mutilazione degli organi genitali femminili*»;
- art. 25 quinquies: «*delitti contro la personalità individuale*», che correlano la responsabilità amministrativa dell'ente alla commissione di illeciti quali la detenzione

di materiale pornografico (prodotto mediante lo sfruttamento sessuale di minori) e le iniziative turistiche volte allo sfruttamento della prostituzione minorile;

- art. 25 sexies: "*reati di abuso del mercato*", che correlano la responsabilità amministrativa dell'ente alla commissione degli illeciti di abuso di informazioni privilegiate e manipolazione del mercato;
- art. 25-septies: «*reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro*»;
- art. 25-octies: «*ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita*», che correla la responsabilità amministrativa dell'ente ad operazioni di trasferimento, occultamento o utilizzo di beni di provenienza illecita;
- art. 25-novies: «*delitti in materia di violazione del diritto d'autore*», ovvero volti all'utilizzo non lecito di materiale protetto da copyright;
- art. 25-decies: «*induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*»;
- art. 25-undecies: «*reati ambientali*», quali lo smaltimento illecito di rifiuti, inquinamento provocato da navi, lo smaltimento di sostanze vietate dalla legge quali lo smaltimento illecito di rifiuti, la distruzione di flora e fauna;
- art. 25-duodecies: «*impiego di cittadini di paesi terzi il cui soggiorno è* irregolare», teso allo sfruttamento di manodopera in condizioni di illegalità;
- art.25 terdecies: "*Razzismo e Xenofobia*";
- "*Reati transnazionali*": introdotti con la legge 16 marzo 2006, n. 146, correlano la responsabilità amministrativa dell'ente a reati quali il riciclaggio e l'associazione per delinquere su scala internazionale;
- art. 25 quaterdecies: "*Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati*";
- Art. 25 quinquiesdecies: "*Reati tributari*", che l'ente per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (artt.

2), il delitto di dichiarazione fraudolenta mediante altri artifici (art. 3), il delitto di emissione di fatture o altri documenti per operazioni inesistenti (art. 8), il delitto di occultamento o distruzione di documenti contabili (art. 10), il delitto di sottrazione fraudolenta al pagamento di imposte (art. 11); con il decreto legislativo 14 luglio 2020, n. 75, la responsabilità dell'ente è stata estesa ai reati di cui agli articoli 4 (dichiarazione infedele), 5 (omessa dichiarazione) e 10 quater (indebita compensazione) del. Dlgs 74/200, qualora tali delitti siano commessi "*nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*";

- Art. 25 sexiesdecies: *"Reati di contrabbando".*

Ai sensi dell'art. 5, D.Lgs. n.231/2001, la responsabilità amministrativa della Società presuppone quindi che sia stato commesso (o tentato) uno dei reati sopra elencati, da una persona fisica funzionalmente collegata all'ente stesso, e che l'atto sia stato commesso «*nel suo interesse o a suo vantaggio*», a meno che l'autore non abbia «*agito nell'interesse esclusivo proprio o di terzi*».

Inoltre, affinché, parallelamente alla responsabilità penale dell'autore del reato (persona fisica), possa profilarsi la responsabilità amministrativa dell'ente, è necessario che il reato sia stato commesso da soggetti che rivestano una posizione apicale all'interno dell'ente o da soggetti in posizione subordinata. Più precisamente, sempre ai sensi dell'art. 5, «l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

a) 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 nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (cosiddetti *soggetti apicali*);

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (cosiddetti *sottoposti)*.

In caso di accertata responsabilità la Società può incorrere in una delle seguenti sanzioni: sanzioni pecuniarie, sanzioni interdittive, confisca e pubblicazione della sentenza.

Le sanzioni interdittive sono costituite da: l'interdizione dall'esercizio dell'attività; la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; il divieto di contrarre con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

Il D.Lgs. n.231/01 prevede, però, l'esclusione della responsabilità della Società nel caso in cui questa abbia adottato ed efficacemente attuato modelli di organizzazione e gestione idonei a prevenire reati della stessa specie di quello verificatosi, oltre ad altre condizioni.

L'art. 6 del Decreto prevede infatti che laddove il reato sia stato commesso da soggetti in posizione apicale, il decreto legislativo stabilisce che l'ente non risponda amministrativamente se fornisce la prova che:

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

Per avere efficacia esimente il modello di organizzazione e gestione deve rispondere all'esigenza di:

- 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 le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di 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.

****

2. Informazioni generali sulla Società

2.1 La Società: STACK EMEA - Italy S.p.A.

La società la cui attuale denominazione sociale è STACK EMEA – Italy è stata costituita il 25 luglio 2014 allo scopo di sviluppare il *business* relativo alla costruzione ed alla gestione di centri elaborazione dati.

In data 26 febbraio 2021, la società americana IPI Partners, LLC ("IPI") ha acquistato da affiliate di Accelero Capital Holdings S.à r.l. il 100% del capitale sociale del socio di controllo della Società, ACDC Holdings S.à r.l. ("ACDC").

L'attività societaria è volta all'elaborazione di tecnologie e di modelli che consentano di acquisire un ruolo di primo piano nella progettazione, nello sviluppo e nella fornitura di servizi di data center "*mission critical*", fornendo ai propri clienti il massimo livello di "*colocation*" e connettività.

In questo quadro, STACK EMEA – Italy S.p.A. è dotata di un Consiglio di Amministrazione plurisoggettivo, composto da cinque membri (di cui un CEO con ampie procure) ed un Presidente del Consiglio di Amministrazione.

La Società – particolarmente attenta alla *compliance* aziendale - ha deciso di adottare un Modello di Organizzazione, Gestione e controllo ai sensi del D.lgs. 231/2001 e di dotarsi di un collegio sindacale.

In aggiunta all'attività di *business* principale, si rilevano al contempo per completezza diverse attività di supporto, come meglio evidenziato nell'oggetto sociale di seguito riportato*:*

"Lo studio, la consulenza, la progettazione, la realizzazione e l'assistenza nel settore dei sistemi informatici e telematici;- la creazione di strutture operative e/o la messa a disposizione e la condivisione di spazi attrezzati all'interno di immobili di proprietà e/o possesso della società, al fine di fornire ad altre società, persone, enti pubblici e/o privati, che operino nel settore del commercio elettronico e della tecnologia informatica, servizi nell'ambito della collocazione e delle tecnologie informatiche, ivi compresa l'installazione, la manutenzione, la gestione, il noleggio ed il commercio, anche attraverso la rivendita, di

hardware e software, la fornitura di servizi di manutenzione ed assistenza divaria natura nei suddetti settori, in particolare attraverso attività di housing, hosting, servers dedicati, web-housing, web-hosting, web-agency, storage, cloud computing, il design, lo sviluppo, l'implementazione, la costruzione e la gestione di progetti di costruzione di data center, l'installazione, la configurazione, la gestione e la manutenzione, diretta ed indiretta, di progetti di networking, consulenza operativa in networking e telecomunicazioni, sicurezza fisica e logica, connettività, traffico di dati e voce, gestione di sistemi operativi, gestione dei networks, backup e restore, disaster recovery, streaming, gestione del traffico voce, gestione del traffico dati, log analysis, analisi di banda, gestione routers, messaging, newsfeed, e la creazione di sistemi autonomi (as);- la promozione e lo sviluppo di prodotti in via telematica;- la commercializzazione in qualsiasi forma dei servizi e dei beni di cui sopra;- la riparazione, la manutenzione e l'installazione di: a) condizionatori, impianti di riscaldamento (elettrici, a gas e petrolio), di condizionamento ed idro termo-sanitari in genere, di bruciatori a gas e gasolio, caldaie, torri di raffreddamento, collettori di energia solare non elettrici, impianti e condotte di ventilazione; b) impianti elettrici ed elettronici in genere civili ed industriali, cablaggi e connessioni elettriche, impianti di illuminazione; c) impianti di collegamento di elettrodomestici e apparecchi elettrici; d) impianti fotovoltaici; e) cablaggi per telecomunicazioni, reti di elaboratori e sistemi televisivi via cavo, incluse le fibre ottiche, parabole satellitari, impianti di segnalazione d'incendio, sistemi di allarme antifurto; f) raccordi per il gas, distributori di vapore; sistemi di spegnimento antincendio inclusi quelli integrati; impianti di sollevamento di persone o cose; impianti di produzione, trasformazione, trasporto, distribuzione e utilizzazione dell'energia elettrica, impianti di messa a terra e contro le scariche atmosferiche, impianti per automazione di porte, cancelli e barriere;- il commercio all'ingrosso e al minuto, anche online, di materiale elettrico, materiale per il riscaldamento, il condizionamento, il trattamento dell'aria egli idro termo-sanitari in genere e di tutto il materiale accessorio ed ausiliario. La società puo' compiere qualsiasi operazione industriale, commerciale, mobiliare, immobiliare e finanziaria compreso il rilascio di fidejussioni e garanzie, comunque connessa, strumentale o complementare al raggiungimento, anche indiretto, degli scopi sociali, fatta eccezione della raccolta del pubblico risparmio e dell'esercizio delle attività

disciplinate dalla normativa in materia di intermediazione finanziaria. Tali attività potranno essere prestate, in Italia o all'estero, direttamente o indirettamente tramite accordi con società terze o tramite la partecipazione nel capitale di società con simile oggetto sociale."

La sede legale e gli uffici direzionali si trovano ad Assago, Via del Bosco Rinnovato 6, mentre il Data Center è situato a Siziano (PV), Via Marche 8/10.

2.2. La "Corporate Governance"

La struttura della "corporate governance" esprime le regole ed i processi con cui si prendono le decisioni in un'impresa, le modalità con cui vengono decisi gli obiettivi aziendali nonché i mezzi per il raggiungimento e la misurazione dei risultati raggiunti. Il sistema di gestione e controllo della STACK EMEA - Italy è quello tradizionale, disciplinato agli artt. 2380 c.c. e seguenti con un Consiglio di Amministrazione con funzioni amministrative di nomina dei soci; la revisione legale è posta in capo ad una società di Revisione.

Vengono sinteticamente descritte di seguito le funzioni degli organi sociali citati:

- Assemblea dei Soci: in linea generale, da un punto di vista normativo, questo organo generalmente delibera sulle materie di esclusiva competenza; esprime indirizzi su ogni questione, tematica, programma proposto dall'organo amministrativo.
- Consiglio di Amministrazione: Il Consiglio di Amministrazione è investito dei più ampi poteri per la gestione della società, senza eccezioni di sorta, ed ha facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione ed il raggiungimento degli scopi sociali, esclusi soltanto quelli che la legge, in modo tassativo, riserva all'assemblea dei soci. Sono inoltre attribuite al consiglio di amministrazione, ferma rimanendo la competenza concorrente dell'assemblea straordinaria a deliberare sulle stesse materie, le deliberazioni concernenti: la fusione nei casi previsti dagli artt. 2505 e 2505-bis codice civile e la scissione nei medesimi casi, richiamati dall'art. 2506-ter codice civile; l'istituzione e la soppressione di sedi secondarie; l'indicazione di quali tra gli amministratori

hanno la rappresentanza della società; la riduzione del capitale in caso di recesso; gli adeguamenti dello statuto a disposizioni normative; il trasferimento della sede sociale nel territorio nazionale.

- Presidente del CdA "Il Presidente del CdA ha la rappresentanza legale della Società ed esercita i poteri conferitigli dal Consiglio di Amministrazione.

Il controllo contabile della Società è affidato ad una società di revisione, e consiste:

- nella verifica periodica della regolare tenuta della contabilità sociale e della corretta registrazione nella contabilità dei fatti di gestione;
- nella verifica del bilancio e, in particolare, della rispondenza dello stesso alla normativa e alle risultanze della contabilità;
- nella formulazione di un giudizio sul bilancio.

Essendo società per azioni, STACK EMEA – Italy ha nominato un Collegio Sindacale, composto da tre membri effettivi e due supplenti. Coerentemente con quanto previsto dagli artt. 2397 ss. C.c., il collegio sindacale ha il compito di vigilare sull'osservanza della legge e dello statuto, sul rispetto dei princìpi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento.

2.3. La Gestione delle risorse finanziarie

L'art. 6, comma 2° lett.c del Decreto esplicitamente statuisce che il Modello debba "i*ndividuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati*".

La gestione delle risorse finanziarie è definita sulla base di principi improntati ad una sostanziale segregazione delle funzioni, tale da garantire che tutti gli esborsi siano richiesti, effettuati e controllati da funzioni indipendenti o soggetti, per quanto

possibile, distinti, ai quali, inoltre, non sono assegnate altre responsabilità tali da determinare potenziali conflitti di interesse. Infine, la gestione della liquidità è ispirata a criteri di conservazione del patrimonio, con connesso divieto di effettuare operazioni finanziarie a rischio, ed eventuale doppia firma per impiego di liquidità per importi superiori a soglie predeterminate.

Nel pieno rispetto degli standard di controllo elaborati da Confindustria, la gestione delle risorse finanziarie della STACK EMEA - Italy avviene in modo trasparente, garantendo la tracciabilità di ogni operazione, la loro congruità, nonché la segregazione delle funzioni coinvolte nei processi pertinenti.

****

3. Il Modello di Organizzazione Controllo e Gestione

3.1 Obiettivi e finalità perseguite nell'adozione del Modello

Attraverso l'adozione del Modello, STACK EMEA - ITALY si propone di perseguire le seguenti principali finalità:

- determinare in tutti coloro che operano in nome e per conto della Società la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, nella commissione di illeciti puniti con sanzioni penali (per le persone fisiche) ed amministrative (per la società);
- rimarcare come tali forme di comportamento illecito siano condannate da STACK EMEA - ITALY , in quanto le stesse sono comunque contrarie alla legge ed ai principi etici;
- consentire alla Società di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi attraverso un'azione di monitoraggio sulle aree di attività a rischio.

Destinatari del Modello e dei principi in esso contenuti sono i membri del CDA, i dirigenti, i dipendenti, i collaboratori, i consulenti, i fornitori, i partner e, più in generale, tutti coloro che, a qualunque titolo, operano nell'ambito delle attività sensibili per conto o nell'interesse di STACK EMEA - ITALY (di seguito "Stakeholders" o "Destinatari").

3.2. Composizione del Modello

Il Modello 231 adottato da STACK EMEA - ITALY è strutturato in modo da integrare il Sistema di Gestione Integrato: esso richiama tutte le procedure interne e le istruzioni operative vigenti in un determinato momento che diventano, in tal modo, parte integrante del modello stesso e la cui violazione determina a sua volta l'applicazione di sanzioni disciplinari come di seguito evidenziato.

Il modello di organizzazione, gestione e controllo di STACK EMEA - ITALY (d'ora in poi anche MOG) è costituito complessivamente dalla seguente documentazione:

- Codice Etico, documento che illustra i valori-guida della Società;

- MOG parte generale, documento che descrive i principi regolatori, i principi generali di comportamento e gli aspetti generali richiesti dal decreto;
- MOG parte speciale, suddivisa in sezioni, nel quale sono individuati i processi sensibili di rilevanza 231 ed i sistemi di controllo adottati, tra cui i protocolli di prevenzione introdotti all'esito della valutazione dei rischi di commissione dei singoli reati;
- la documentazione operativa interna, le procedure in essa indicate, le istruzioni operative, il DVR, nonché il Manuale del Sistema di Gestione Integrato che la Società ha adottato e provvederà ad adottare;
- il sistema sanzionatorio conseguente al mancato rispetto dell'impianto normativo della società e del modello in generale;
- i processi di formazione e informazione delle regole aziendali;
- i flussi di informazione verso l'Organismo di Vigilanza
- la procedura Whistleblowing.

3.3. I principi regolatori del Modello

Nella definizione, costruzione ed applicazione del modello si sono osservati i seguenti principi regolatori:

- una chiara e formalizzata assegnazione di poteri e responsabilità, coerente con le mansioni attribuite;
- la separazione delle funzioni (ove possibile), per cui l'autorizzazione ad effettuare un'operazione deve essere assunta da soggetto diverso da chi contabilizza, esegue operativamente o controlla l'operazione;
- la formalizzazione di regole comportamentali idonee a garantire l'esercizio delle attività aziendali;
- la c.d. "tracciabilità", volta a garantire che ogni operazione, transazione e/o azione sia verificabile, documentata, coerente e congrua.

Punti cardine del Modello sono, oltre ai principi già indicati:

- l'attività di diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;

- la mappatura delle aree di attività a rischio dell'azienda, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- l'attribuzione all'Organismo di Vigilanza di specifici compiti di controllo sull'efficace e corretto funzionamento del Modello;
- la definizione di flussi informativi a carico delle funzioni aziendali verso l'Organismo di vigilanza;
- la specificazione di principi generali di comportamento a cui i destinatari delle parti speciali richiamate, devono attenersi;
- la verifica dei comportamenti aziendali, mediante audit periodici mirati alla verifica del funzionamento del Modello con conseguente aggiornamento periodico (controllo ex post).

3.4. La metodologia adottata per l'implementazione del Modello

L'attività di realizzazione del modello, conformemente a quanto suggerito dalle Linee Guida Confindustria aggiornate al 2021 e dal D.Lgs. n.231/01 si è svolta nel seguente modo:

- Identificazione dei processi e delle relative interazioni attraverso la mappatura dei processi;
- Risk Assessment e Gap Analysis: attraverso l'analisi documentale e l'esecuzione di interviste con i soggetti deputati ad assumere il ruolo di responsabili dei processi sono state preliminarmente evidenziate le attività esposte al rischio di illecito;
- Individuazione dei sistemi di controllo e definizione dei protocolli a presidio dei processi sensibili;
- Determinazione del sistema disciplinare;
- Disciplina dell'Organismo di Vigilanza deputato al controllo sull'efficace e corretto funzionamento del Modello;
- Attuazione di una procedura di Whistleblowing.

3.5. Principi generali del SCI

Il Sistema di Controllo Interno di STACK EMEA - ITALY è costituito dall'insieme delle regole, delle procedure, delle istruzioni operative e della struttura organizzativa ed è

volto a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi aziendali, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

Gli elementi costitutivi del Sistema di Controllo Interno sono:

- il Codice Etico;
- il sistema di Deleghe e Procure;
- la Struttura Organizzativa ed il controllo gerarchico;
- la Documentazione organizzativa, ovvero gli Organigrammi, le Procedure interne, le Certificazioni volontarie, i Manuali e le Istruzioni operative che la Società provvederà ad adottare, a valle del completamento della Sua organizzazione.

****

4. L'esposizione al rischio

4.1. Premessa metodologica

I processi definiti all'interno di STACK EMEA - ITALY per un'efficace ed efficiente erogazione del servizio possono essere esposti al rischio di commissione dei reati previsti dal D.lgs. n.231/2001 secondo tre modalità distinte:

- ***esposizione diretta***, se l'esecuzione delle attività all'interno del processo è di per sé stessa esposta al rischio di commissione di illecito. Ad esempio, la richiesta di una concessione edilizia, espone il personale incaricato direttamente ai reati di corruzione.

- ***esposizione strumentale***, se il processo di per sé stesso non è esposta a rischio di illecito, ma costituisce il modo per integrare una delle ipotesi illecite di cui al decreto. Ad esempio:

    - l'assunzione di dipendenti legati a figure della Pubblica Amministrazione può costituire la "dazione" attraverso la quale si perfeziona il reato di corruzione per un atto contrario ai doveri d'ufficio;

    - la conclusione di contratti di consulenza può costituire la modalità attraverso la quale costituire fondi occulti da utilizzare per scopi di natura illecita;

    - la conclusione di simulati contratti di approvvigionamento di beni o di servizi può costituire il mezzo per la costituzione di fondi occulti;

    - concludere transazioni/conciliazioni simulate in modo assoluto o relativo, può costituire un modo per la costituzione di riserve occulte liquide;

    - sponsorizzazioni, donazioni simulate possono giustificare un flusso di denaro in uscita finalizzato a creare una riserva occulta liquida.

- ***nessuna esposizione***, se l'attività o il processo non presentano una significativa esposizione al rischio di commettere determinate categorie di reati.

4.2. I Processi sensibili e i Reati presupposto ex D.lgs. n.231/01

Alla luce dell'analisi di rischio svolta, ai fini della predisposizione del presente Modello, si considerano concretamente rilevanti per la Società i seguenti reati, in ragione della oggettiva possibilità di commissione nelle macro-aree di riferimento, nello svolgimento dei processi e delle attività sensibili pertinenti ai primi. Come emerso in fase di *risk assessment,* le aree analizzate riguardano i processi che la Società andrà ad implementare una volta conclusa la costruzione del *Data Center* ed iniziata la concreta gestione operativa della Società, coerentemente con il modello di *business* posto a fondamento della specifica iniziativa imprenditoriale affidata alla Società.

Reati Presupposto D.Lgs. n.231/2001	**Macro-aree**	**Processi e attività sensibili**
Reati contro la Pubblica Amministrazione (art. 25)	Corporate Governance	• Identificazione ed attribuzione di poteri e deleghe • Brand Management
	Gestione Risorse finanziarie	• Tax & Finance • Accounting • Bilancio • Tesoreria • Operazioni con parti correlate • Gestione contenzioso
	Risorse umane	• Selezione, inserimento e gestione amministrativa del personale • Definizione del sistema premiante
	Approvvigionamenti e Procurement	• Gestione acquisti e fornitori • Gestione incarichi professionali e consulenze • Gestione contratti
	Compliance	• Compliance SSL • Gestione ambientale
	Commerciale	• Contratti con pubblica

		amministrazione
Delitti informatici (art. 24-bis)	IT	• Disegno e gestione infrastruttura HeS • Incident Management • Data Security System
Delitti di criminalità organizzata (art. 24-ter) Reati transnazionali Art. 3 - L. 146/2006	Gestione Risorse finanziarie	• Operazioni con parti correlate • Tax & Finance • Accounting • Tesoreria • Bilancio
	Processi di business	• Commerciale
	Risorse umane	• Selezione, inserimento e gestione amministrativa del personale
	Approvvigionamenti e Procurement	• Gestione acquisti e fornitori
Reati societari (art. 25-ter)	Corporate Governance	• Brand Management
	Gestione Risorse finanziarie	• Tax & Finance
	Processi di business	• Commerciale
	Approvvigionamenti e Procurement	• Gestione acquisti e fornitori
Reati in materia di SSL (art. 25-septies)	Compliance	• Gestione Compliance HSE
Reati ambientali (art. 25-undecies)	Compliance	• Gestione Compliance volontaria
Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies)	Gestione Risorse finanziarie	• Tax & Finance • Tesoreria • Accounting • Operazioni con parti correlate
	Approvvigionamenti e Procurement	• Gestione acquisti e fornitori

	Processi di business	• Commerciale
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies. Legge 6 novembre 2012, n. 190)	Risorse umane	• Selezione, inserimento e gestione amministrativa del personale
Reati Tributari (art. 25 quinquiesdecies)	Processi di business	• Commerciale
	Gestione Risorse finanziarie	• Tax & Finance • Accounting • Bilancio • Tesoreria • Operazioni con parti correlate • Gestione contenzioso
	Approvvigionamenti e Procurement	• Gestione acquisti e fornitori • Gestione incarichi professionali e consulenze • Gestione contratti
Reati di contrabbando (art. 25 sexiesdecies)	Approvvigionamenti	• Gestione acquisti e fornitori • Gestione contratti

I risultati dell'attività di mappatura hanno consentito di:

- identificare le unità organizzative della Società che, in considerazione dei compiti e delle responsabilità attribuite, potrebbero potenzialmente essere coinvolte nelle attività a rischio reato;
- individuare le principali fattispecie di rischio/reato;
- delineare le possibili modalità di realizzazione dei comportamenti illeciti.

Di seguito sono elencati i reati presupposto ex D.lgs. n.231/01 che hanno assunto diretta rilevanza per STACK EMEA - ITALY; per la dettagliata indicazione, specificazione ed analisi degli stessi si richiama l'indice allegato che costituisce parte integrante del MOG.

4.2.1. I reati contro la Pubblica Amministrazione ex artt.24 e 25 D.lgs. n.231/2001.

L'esposizione al rischio

Pur in attesa di una concreta operatività societaria, è verosimile ritenere che i clienti di STACK EMEA - ITALY saranno quasi esclusivamente costituiti da soggetti privati ciò nondimeno, è apparso comunque utile considerare – in via prudenziale - anche la possibile partecipazione a gare pubbliche e/o la conseguente stipulazione di rapporti contrattuali con la P.A. inerenti allo svolgimento dell'attività sociale, con un contestuale rischio di commissione (sia pur contenuto) di reati contro la P.A.

Inoltre, le ipotesi di reato previste dagli artt. 24 e 25 D.lgs. n.231/01 possono trarre spunti criminogeni da altri occasionali rapporti con la Pubblica Amministrazione, ad esempio in relazione alla gestione dei provvedimenti autorizzativi/concessori (ad es. provvedimenti di natura edilizia per il Data Center di Siziano), durante le visite ispettive, ovvero nei rapporti con l'Amministrazione finanziaria; pertanto, alcuni dei processi sensibili sono risultati meritevoli di presidio in quanto, benché non assumano rilevanza diretta, potrebbero costituire la via attraverso la quale l'ente potrebbe distrarre risorse finanziarie da destinare agli illeciti in esame (ad es. assunzione di un candidato o scelta di un fornitore come prezzo da pagare in ossequio ad un accordo corruttivo).

Si rimanda all'allegato elenco reati e *case study* per la descrizione delle fattispecie previste dagli artt. 24 e 25 del Decreto. I Principi e le regole di condotta sottoelencati rappresentano un utile presidio finalizzato a ridurre i rischi di commessione dei reati contro la P.A.

Principi generali di comportamento e regole di condotta

Si prevede l'espresso divieto, a carico dei Destinatari del presente Modello, di porre in essere comportamenti:

- tali da integrare le fattispecie di reato di cui al presente paragrafo;

- non conformi con i principi e le prescrizioni contenute nel presente Modello, del Codice Etico, delle Norme comportamentali o con le procedure aziendali;

- tali da favorire qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

A tale scopo è fatto divieto in particolare di:

a) compiere azioni o tenere comportamenti che siano o possano essere interpretati come corruttive, favori illegittimi, comportamenti collusivi, sollecitazioni, dirette o mediante terzi, di privilegi per sé o per altri rilevanti ai fini della commissione dei reati di cui al Decreto;

b) distribuire omaggi e regali a Pubblici ufficiali o ad Incaricati di pubblico servizio, ovvero a coloro che con gli stessi hanno rapporti privilegiati o millantano di averne;

c) esercitare indebite pressioni o sollecitazioni su pubblici ufficiali o soggetti terzi in vista del compimento di attività inerenti all'ufficio;

d) presentare dichiarazioni non veritiere a organismi pubblici nazionali, ed esteri al fine di conseguire autorizzazioni, licenze e provvedimenti amministrativi di qualsivoglia natura;

f) presentare dichiarazioni non veritiere a organismi pubblici nazionali o esteri al fine di conseguire finanziamenti, contributi o erogazioni di varia natura, sconti fiscali;

g) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;

h) effettuare o promettere, in favore dei clienti, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito;

i) riconoscere, in favore dei Fornitori, Appaltatori, Agenti, Consulenti esterni e/o Collaboratori, compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;

l) concludere contratti di consulenza con soggetti interni alla Pubblica Amministrazione in base ai quali si potrebbe minare l'imparzialità e il buon andamento della Pubblica Amministrazione stessa;

m) assumere soggetti legati da rapporti con clienti pubblici e privati di STACK EMEA - ITALY;

n) accedere fraudolentemente ai sistemi informatici della Pubblica Amministrazione per ottenere o modificare dati o informazioni nell'interesse o a vantaggio della Società;

o) prospettare od offrire alle pubbliche amministrazioni lo svolgimento di prestazioni che STACK EMEA - ITALY non è in grado di svolgere adeguatamente;

p) richiedere alle pubbliche amministrazioni il pagamento di prestazioni di cui non sia stata preventivamente verificata la corretta e regolare esecuzione.

Ai fini dell'attuazione dei divieti suddetti, dovranno rispettarsi le regole di seguito indicate:

- i rapporti con funzionari della Pubblica Amministrazione devono essere dunque gestiti esclusivamente da persone opportunamente identificate e dotate di idonei poteri e deleghe;

- tutti coloro che materialmente intrattengono rapporti con la Pubblica Amministrazione per conto della Società devono godere di un'autorizzazione in tal senso da parte della Società stessa;

- tutti i dipendenti di STACK EMEA – ITALY dovranno attenersi scrupolosamente e rispettare eventuali limiti previsti nelle deleghe o procure conferite dalla Società;

- i rapporti con la Pubblica Amministrazione devono avvenire nell'assoluto rispetto delle leggi, delle normative vigenti, dei principi di lealtà e correttezza, nonché dei principi contenuti nel Modello e nel Codice Etico, in qualunque fase di gestione del rapporto;

• gli incarichi conferiti ai Collaboratori, Consulenti esterni, Fornitori devono essere redatti per iscritto, con indicazione del compenso pattuito, del dettaglio della prestazione e dei tempi di esecuzione;

• le dichiarazioni rese a organismi pubblici nazionali o esteri per il rilascio/rinnovo di autorizzazioni/licenze di qualsivoglia natura, ovvero conseguimento di finanziamenti, contributi e/o erogazioni o sconti fiscali di varia natura devono contenere elementi assolutamente veritieri e devono essere autorizzate da soggetti dotati di idonei poteri; inoltre, in caso di ottenuto conferimento/ottenimento degli stessi, deve essere mantenuto apposito rendiconto circa l'utilizzo del finanziamento/contributo;

• nessun tipo di pagamento non adeguatamente documentato ed autorizzato può esser effettuato;

• tutti i dipendenti STACK EMEA - ITALY e i Collaboratori sono tenuti a rispettare le procedure, direttive e policy aziendali applicabili alle attività svolte in particolare nell'ambito dei Processi Sensibili;

• la scelta dei Fornitori, Appaltatori, Agenti, Consulenti esterni e/o Collaboratori deve avvenire sulla base di criteri di serietà e competenza del professionista/collaboratore e l'assegnazione degli incarichi deve avvenire sulla base di un processo decisionale che garantisca la segregazione dei compiti e delle responsabilità;

• i Fornitori, Appaltatori, Agenti, Consulenti esterni e/o Collaboratori dovranno prendere visione del Modello e del Codice Etico ed impegnarsi a rispettarne le previsioni, secondo quanto stabilito in specifiche clausole, inserite nel/aggiunte al contratto stipulato tra gli stessi e la Società, che prevedono, in ipotesi di violazione di tali previsioni, la risoluzione del suddetto contratto.

• i contratti con i Fornitori e gli Appaltatori, nonché gli incarichi con gli Agenti, Consulenti e/o Collaboratori devono essere definiti per iscritto, con evidenziazione di tutte le condizioni ad essi sottese (con particolare riferimento alle condizioni

economiche concordate), nonché della dichiarazione di impegno a rispettare il Modello e il Codice Etico e delle conseguenze nel caso di violazione;

- i contratti con i Fornitori e gli Appaltatori, nonché gli incarichi con gli Agenti, Consulenti esterni e/o Collaboratori devono essere approvati dai soggetti della Società muniti degli appositi poteri di firma;

- le proposte formulate per conto di STACK EMEA – ITALY devono essere preventivamente oggetto di adeguata verifica tecnica;

- In caso di assunzione di risorse, dovrà essere richiesta un'autodichiarazione di assenza di carichi pendenti, di precedenti penali e di misure antimafia di cui al D.lgs. 159/2011, nonché una dichiarazione concernente lo status di persona politicamente esposta o che ha rapporti di parentela con esponenti PA, con altri dipendenti, con clienti o con fornitori.

4.2.2. I Reati informatici, reati di falso in materia di marchi, brevetti, segni distintivi e reati commessi in violazione della Legge sul diritto d'autore ex art.24 bis, 25 bis e 25 novies D.lgs. n.231/2001.

L'esposizione al rischio

Con riferimento ai reati in esame, è opportuno svolgere un distinguo tra l'attività di business e le attività generiche di supporto al business.

Con riferimento alla prima, l'attività di STACK EMEA - ITALY è sostanzialmente costituita dal mettere a disposizione dei propri clienti, all'interno del Data Center, aree protette dove collocare i propri server o altra strumentazione elettronica nei quali è contenuta documentazione informatica di diversa natura (in alcuni casi garantendo anche la connettività Internet). La società non svolge e non deve svolgere alcun controllo su quanto digitalmente custodito nei server dei clienti, e non ne conosce il contenuto.

La gestione dei Rack (struttura che custodisce la strumentazione del cliente) è, infatti, rimessa esclusivamente al cliente ed ai propri tecnici. Nessun intervento manutentivo, se non concordato con il cliente, viene svolto dal personale di STACK EMEA - ITALY sulle

apparecchiature di quest'ultimo. Tuttavia, mantenendo l'azienda un diretto ed immediato contatto diretto con i dati informatici e le apparecchiature del cliente, astrattamente assumono pertinenza alcuni dei reati informatici in esame, quali ad esempio l'accesso abusivo ad un sistema informatico o telematico, Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. Tuttavia, gli illeciti di tale natura, in considerazione della continua ed intensa attività di presidio e controllo (per numero di risorse aziendali impiegate e per la diuturna attività di misurazione e monitoraggio) svolta dalla società, rende estremamente improbabile la consumazione degli illeciti in esame, sia da parte di dipendenti della azienda e sia da parte di terzi che, in modo autorizzato, accedono all'interno del Data Center.

Con riferimento, invece, alle attività generiche di supporto al business, per la tipologia dell'attività svolta e la struttura organizzativa dell'azienda, l'area IT di STACK EMEA - ITALY risulta ovviamente quella astrattamente più esposta alla classe dei reati informatici: ancorché infatti la loro commissione diretta possa avvenire in teoria da parte del personale di ogni area dell'azienda, è la funzione IT che, definendo le caratteristiche di sicurezza dell'intera infrastruttura fisica e logica della Società, può creare le condizioni di vulnerabilità atte al concretizzarsi della minaccia di illecito; ed invero stante la presenza di importanti presidi di controllo adottati dalla società che ne rendono, di fatto, impossibile la consumazione, questi illeciti (ad interesse o a vantaggio della azienda stessa) possono consumarsi solo con il concorso della funzione IT. In quest'ultimo caso sarebbero astrattamente ipotizzabili (per quanto in concreto improbabili) la consumazione i reati di: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art 617 quater, c.p.) di danneggiamento di informazioni, dati e programmi informatici, ancorché utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (artt. 635 bis e 635 ter, c.p.) nonché di danneggiamento di sistemi informatici o telematici e danneggiamento di sistemi informatici o telematici di pubblica utilità (artt. 635 quater e 635 *quinquies*) di frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640 *quinquies*) e di falsa dichiarazione o attestazione al certificatore di firma elettronica (art.495 bis) e falsificazioni informatiche (art. 491 bis). Analogamente potrebbero

assumere altresì rilevanza gli illeciti presupposto di cui all'articolo 25-novies decreto legislativo 8 giugno 2001, n. 231 (Violazione diritti d'autore) concretantisi nell'uso di programmi informatici senza licenza.

Infine, il Decreto-legge 105/2019, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" e convertito con modificazioni dalla Legge 133/2019, ha inserito all'interno dell'art. 25 *bis* il delitto previsto dall'art. 1, comma 11, dello stesso Decreto. Tale delitto sanziona "*Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto*".

Tale reato non appare direttamente riferibile all'attività comunemente svolta da STACK EMEA - ITALY, la quale non rientra allo stato tra i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. Ciò nondimeno, a fronte di possibili rapporti commerciali con tali operatori, si è comunque ritenuto di considerare il (limitato) rischio di concorso in comportamenti illeciti relativi ad altre aziende ovvero di comunicazione di false informazioni alle autorità richiedenti, con conseguente implementazione dei presidi già previsti nel settore della sicurezza informatica.

Principi generali di comportamento

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla rubrica, i Destinatari coinvolti nello svolgimento delle Attività Sensibili nelle Aree a Rischio Reato individuate, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali:

a) astenersi dal tenere comportamenti tali integrare le fattispecie previste dai suddetti reati di criminalità informatica, ovvero da comportamenti che, sebbene

risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possono potenzialmente diventarlo;

b) rispettare le regole di condotta generale, i principi di controllo e le prescrizioni specifiche formulate nel presente Modello;

c) rispettare le norme, le policy e le procedure aziendali che disciplinano l'accesso e l'utilizzo dei sistemi e degli applicativi informatici della Società e dei clienti, nonché le procedure adottate dalla Società in materia di protezione dei dati personali;

d) tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla gestione dei rapporti con i fornitori/clienti;

f) attenersi alle eventuali policy adottate dalla Società contenenti principi cui attenersi al fine di rispettare i diritti di proprietà industriale di terzi e tutelare quelli della Società;

g) prevedere l'inserimento sistematico di una "clausola 231" in tutti i contratti con Consulenti, Fornitori, ed altri terzi in base alla quale il soggetto terzo dichiara di aver preso visione dei contenuti del Modello, del Codice Etico e di impegnarsi a rispettare le prescrizioni in essi esplicitate, a pena di risoluzione del contratto;

i) adeguare costantemente l'organizzazione aziendale ed i servizi offerti alla clientela agli standard di sicurezza informatica richiesti dalle normative di settore e dalle *best practice* di riferimento;

l) in caso di rapporti commerciali con soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, astenersi da ogni interferenza nelle comunicazioni con i soggetti pubblici di controllo, comunicando costantemente al Committente dei dati trasparenti, corretti ed aggiornati in modo da evitarne qualsiasi possibile strumentalizzazione;

m) collaborare ad ogni eventuale accertamento giudiziario o amministrativo, astenendosi dal divulgare notizie coperte da segreto.

Ai Destinatari è vietato:

- utilizzare periferiche di archiviazione di massa (cd, dvd riscrivibili, chiavette usb) se non espressamente autorizzate;

- utilizzare programmi diversi da quelli installati nel pc in dotazione, ovvero installare autonomamente programmi provenienti dall'esterno;

- navigare in Internet in siti non attinenti allo svolgimento delle mansioni assegnate;

- navigare in Internet utilizzando una connessione diversa da quella aziendale;

- effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili;

- scaricare software gratuiti e shareware prelevati da siti Internet;

- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica, ovvero di natura pedopornografica;

- l'uso e la navigazione su siti di tipo x-rated (siti per adulti), casinò virtuali, webchat, social network;

- scaricare/scambiare materiale coperto da diritto d'autore;

- usare il servizio per scopi illegali, per inviare e ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso;

- aprire allegati di posta elettronica ambigui o di incerta provenienza.

4.2.3. I Reati di criminalità organizzata ex art. 24-ter D.lgs. n.231/01 - Reati transnazionali Art. 3 L. n.146/2006

L'esposizione al rischio

L'art. 1 della Legge 16 marzo 2006 n. 146 ha ratificato e dato esecuzione in Italia alla Convenzione Internazionale e ai Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001 (Convenzione di Palermo). L'art. 10 di quest'ultima ha introdotto la responsabilità amministrativa degli enti in relazione a determinate ipotesi di reato transnazionale.

L'articolo 3 della Legge 16 marzo 2006 n. 146, rubricato "Definizione di reato transnazionale", così recita:

> *1. Ai fini della presente legge si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:*
> *a) sia commesso in più di uno Stato;*
> *b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;*
> *c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;*
> *d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.*

In ragione dell'articolo 10 della Legge 16 marzo 2006 n. 146, e dell'art.24 ter D.lgs. n.231/01, la responsabilità dell'ente può sorgere allorché, soddisfatti i requisiti del sopra citato art.3, vengano consumati i reati di cui all' art. 378 c.p. (Favoreggiamento personale), art. 291-quater del D.P.R. 23 gennaio 1973, n. 43 (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri), art. 12, comma 3, 3-bis, 3-ter e 5 del D.lgs. 25 luglio 1998, n. 286 (Delitti in materia di immigrazione clandestina), di associazione per delinquere (art. 416 c.p.), associazione di tipo mafioso (art. 416-bis c.p.) e di associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74 DPR n. 309 del 1990).

Le ultime tre fattispecie di reato assumono rilevanza nel riconoscimento della responsabilità amministrativa delle persone giuridiche non solo se caratterizzate dal requisito della transnazionalità, ma – come accade per la generalità degli illeciti rilevanti per il D. Lgs. 231/01 – anche se realizzate esclusivamente nel territorio dello stato italiano.

La consumazione di alcuni dei reati sopra indicati in modo da coinvolgere la società è, di fatto, impossibile. Invece, in ragione del carattere di internazionalità che distingue STACK EMEA - ITALY , alcuni di essi sono invece astrattamente rilevanti e la loro consumazione afferisce alla gestione dei rapporti con persone fisiche o giuridiche aventi sede od operanti in Paesi considerati a rischio, alla gestione di operazioni finanziarie o transazioni verso paesi considerati a rischio.

Principi generali di comportamento

Nell'espletamento delle proprie funzioni, oltre alle regole di cui al presente Modello, i Destinatari devono, in generale, conoscere e rispettare le norme inerenti la prevenzione dei reati di criminalità organizzata e i reati c.d. transnazionali.

In particolare, ai Destinatari è fatto espresso divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, considerati individualmente o collettivamente, tali da integrare, in maniera diretta o indiretta, le fattispecie di reato considerate dall'articolo 24-ter del D.lgs. n. 231/01 e dall'art. 10, Legge n. 146/2006;
- fornire, direttamente o indirettamente, fondi a favore di soggetti che perseguono, direttamente o in qualità di prestanome, finalità di criminalità organizzata transnazionale, agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche.
- istituire rapporti contrattuali (connessi all'erogazione di servizi professionali o all'acquisto di beni e servizi, etc.) ovvero effettuare qualsivoglia operazione commerciale e/o finanziaria, sia direttamente che per il tramite di interposta persona, con soggetti - persone fisiche o giuridiche - i cui nominativi siano contenuti nelle Black List, disponibili presso la Banca d'Italia, o da soggetti da questi ultimi controllati, quando tale rapporto di controllo sia noto. A tale proposito, è necessario che vengano svolte tutte le attività necessarie alla identificazione della clientela e alla verifica dell'assenza dei conflitti di interesse, nonché di sospetti in ambito terroristico;

- effettuare prestazioni in favore di terzi, italiani o stranieri, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- riconoscere compensi in favore di terzi, italiani o stranieri, che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
- ricevere compensi per forniture o prestazioni inesistenti o che esulano dalla ordinaria attività d'impresa;
- erogare liberalità a favore di enti e soggetti inseriti nelle *black list* internazionali;
- assumere personale risultante dalle *black list* internazionali.

Alla luce di quanto sopra, al fine di prevenire la commissione dei reati previsti all'art. 24-ter del D.lgs. n. 231/01 e dall'articolo 10 della Legge n. 146/06 e ritenuti rilevanti per la società, quest'ultima adotta norme di comportamento e regole improntate a:

1) verificare che qualunque transazione finanziaria presupponga la previa conoscenza del beneficiario o erogante e della relativa somma di denaro;

2) verificare che gli incarichi di rilevante valore siano conclusi con le persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli ed accertamenti;

3) verificare l'attendibilità commerciale e professionale dei fornitori e partners commerciali/finanziari;

4) verificare che i dati raccolti relativamente ai rapporti con terzi siano completi ed aggiornati sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del profilo;

5) verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari ed ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;

6) espletare i controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede

legale della società controparte, degli istituti di credito utilizzati e di eventuali schermi societari utilizzati per transazioni o operazioni straordinarie;

7) effettuare periodici controlli interni sulla tesoreria;

8) adottare adeguati programmi di formazione del personale.

4.2.4. I reati societari ex art. 25 ter D.Lgs.n.231/01.

La tipologia dei reati in oggetto è di particolare rilevanza sia per la frequenza di attività che espongono a rischio la Società che per la molteplicità degli interessi che si vuole proteggere, quali la tutela dell'integrità del patrimonio aziendale, la tutela dei soci e dei creditori, la concorrenza leale, etc etc. Diverso è il caso della corruzione tra privati, reato che si perfeziona allorquando "*gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro od altre utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società*".

L'esposizione al rischio

Alla luce dell'attuale organizzazione aziendale, il processo di contabilità e di elaborazione dei dati di bilancio sarà inevitabilmente oggetto di esternalizzazione, con conseguente affidamento del controllo contabile ad una società esterna, implementando in tal modo uno specifico presidio idoneo a limitare e circoscrivere la possibilità di anomalie e/o di irregolarità contabili di natura dolosa. Ciò nonostante, la possibile commissione di reati societari (false comunicazioni sociali, false comunicazioni sociali in danno dei soci o dei creditori, impedito controllo, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, illecita influenza sull'assemblea, formazione fittizia del capitale, operazioni in pregiudizio dei creditori, corruzione tra privati) ha in ogni caso suggerito la doverosa adozione di regole di condotta, tali da ridurre ulteriormente il rischio di commissione di reati societari.

Una volta sviluppata la propria organizzazione aziendale, sarà inoltre possibile adottare uno specifico protocollo relativo alle operazioni con parti correlate, integrando le forme di controllo attualmente già esistenti nell'ambito delle stesse.

Principi generali di comportamento e regole di condotta

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla rubrica, i Destinatari coinvolti nello svolgimento delle Attività Sensibili sono tenuti al rispetto dei seguenti principi generali e regole di condotta, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali:

- i Destinatari devono osservare una condotta improntata a principi di integrità, correttezza e trasparenza nell'attività di formazione del bilancio, delle relazioni e delle altre comunicazioni sociali previste dalla legge, in modo da fornire ai soci e al pubblico informazioni veritiere e corrette sulla situazione economica, patrimoniale e finanziaria di STACK EMEA - ITALY nel rispetto di tutte le norme di legge, regolamentari e dei principi contabili applicativi. Pertanto, è vietato indicare o inviare per l'elaborazione o l'inserimento in dette comunicazioni, dati falsi, artefatti, incompleti o comunque non rispondenti al vero, sulla situazione economica, patrimoniale o finanziaria della Società. È fatto inoltre divieto di porre in essere attività e/o operazioni volte a creare disponibilità extracontabili ovvero volte a creare "fondi neri" o "contabilità parallele". I soggetti che intervengono nel procedimento di stima devono attenersi al rispetto del principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti, fornendo ogni informazione complementare che sia necessaria a garantire la veridicità del documento. Il bilancio deve inoltre essere completo sotto il profilo dell'informazione societaria e deve contenere tutti gli elementi richiesti dalla legge. Analoga correttezza è richiesta agli amministratori, nella redazione di tutte le altre comunicazioni imposte o comunque previste dalla legge e dirette ai soci, affinché le stesse contengano informazioni chiare, precise, veritiere e complete;

- i Destinatari devono osservare una condotta tesa a garantire il regolare funzionamento di STACK EMEA - ITALY, e la corretta interazione tra i suoi organi sociali, assicurando ed agevolando ogni forma di controllo sulla gestione sociale, nei modi

previsti dalla legge, nonché la libera e regolare formazione della volontà. In tale prospettiva, è vietato:

a) impedire od ostacolare in qualunque modo, anche occultando documenti o utilizzando altri idonei artifici, lo svolgimento delle attività istituzionali di controllo e di revisione;

b) determinare o influenzare illecitamente l'assunzione delle delibere assembleari, ponendo a tal fine in essere atti simulati o fraudolenti che si propongano di alterare artificiosamente il normale e corretto procedimento di formazione della volontà assembleare.

- i Destinatari devono garantire il puntuale rispetto di tutte le norme di legge che tutelano l'integrità e l'effettività del capitale sociale, al fine di non creare nocumento alle garanzie dei creditori e, più in generale, ai terzi;

- all'organo amministrativo è vietato restituire, anche simulatamente, i conferimenti ai soci o liberarli dall'obbligo di eseguirli, fatte salve ovviamente le ipotesi di legittima riduzione del capitale sociale;

- all'organo amministrativo è vietato ripartire utili o acconti su utili non effettivamente conseguiti, o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite;

- all'organo amministrativo è vietato effettuare riduzioni del capitale sociale o fusioni con altre società o scissioni in violazione delle norme di legge, con ciò cagionando un danno ai creditori;

- all'organo amministrativo è vietato formare o aumentare fittiziamente il capitale sociale mediante attribuzioni di azioni per somma inferiore al loro valore nominale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio sociale in caso di trasformazione;

- ai Destinatari è vietato compiere azioni o tenere comportamenti nei confronti di esponenti di società (siano esse clienti, fornitori, consulenti ecc.) che siano o possano essere interpretati come pratiche di corruzione, favori illegittimi, comportamenti

collusivi, sollecitazioni, dirette o mediante terzi, di privilegi per sé o per altri rilevanti ai fini della commissione del reato di corruzione tra privati;

- ai Destinatari è vietato distribuire o ricevere omaggi commerciali, regali o altre utilità (inclusi pasti, viaggi e attività di intrattenimento) che possano costituire violazione di leggi o regolamenti o siano in contrasto con il Codice Etico. In particolare, non è consentito offrire denaro o utilità di qualsiasi tipo (promesse assunzione, etc.) o compiere atti di cortesia commerciale, salvo che si tratti di utilità di modico valore e sempre che comunque non possano essere in alcun modo interpretate quale strumento per influenzarli nell'espletamento dei loro doveri o per indurli a violare i loro obblighi d'ufficio o di fedeltà per ricevere favori illegittimi e/o per trarne indebito vantaggio. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato a consentire le prescritte verifiche;

- ai Destinatari è vietato riconoscere, in favore dei Fornitori, consulenti e/o collaboratori esterni, partner commerciali, Agenti, Appaltatori compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente nel settore di attività interessato;

- Per quanto concerne la predisposizione delle comunicazioni ai soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della società (bilancio d'esercizio, relazioni trimestrali e semestrali), i documenti devono essere redatti sulla base di procedure o istruzioni operative che determinano con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili. È inoltre necessario che la trasmissione di dati ed informazioni avvenga attraverso un sistema che consenta la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;

- La documentazione e la comunicazione di tutti i dati e le informazioni soggette a controllo da parte di soci, sindaci ed eventualmente della società di revisione contabile deve avvenire in modo trasparente, senza che siano frapposti ostacoli allo svolgimento delle attività di controllo o di revisione;

4.2.5. I reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro ex art.25 septies D.Lgs. n.231/01

Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il modello organizzativo e gestionale di cui al primo punto deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra riportate.

Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di

idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti.

L'esposizione al rischio

Premesso che allo stato attuale STACK EMEA - ITALY risulta ancora sprovvista di dipendenti, la stessa dovrà conseguentemente procedere, all'avvio dell'attività operativa, alla predisposizione di un documento di valutazione rischi con l'ausilio di una consulenza esterna ed all'adozione di un sistema di gestione integrato volto a monitorare adeguatamente i rischi SSL (oltre che ambientali) ed a limitare, per quanto possibile, in ragione delle conoscenze tecniche attuali, il pericolo per la salute dei propri dipendenti e di coloro che accedono nelle aree di sua competenza.

Il modello organizzativo non potrà pertanto sostituirsi alle prerogative e responsabilità di legge disciplinate in capo ai soggetti individuati dal D.Lgs. n.81/08, dovendo invece costituire un presidio ulteriore di controllo e di verifica dell'esistenza, efficacia ed adeguatezza, della struttura del sistema di gestione per la tutela della salute e sicurezza sui luoghi di lavoro.

Principi generali di comportamento

Tutti dipendenti e Collaboratori della Società, nei rispettivi ambiti e per la propria competenza, sono tenuti a:

• rispettare le norme, gli obblighi e i principi posti dalla normativa vigente e dalle norme/linee guida in materia di salute e sicurezza;

• rispettare i principi generali di condotta e comportamento, i principi di controllo e i principi specifici formulate nel presente Modello;

• promuovere il rispetto delle suddette norme, regole e principi e assicurare gli adempimenti in materia di salute e sicurezza sul lavoro;

• adottare una condotta di massima collaborazione e trasparenza nei rapporti con gli enti pubblici competenti in materia salute e sicurezza sul lavoro, sia in fase di stesura e comunicazione di eventuali dichiarazioni, sia in occasione di accertamenti/verifiche ispettive;

• promuovere l'informazione e formazione interna in tema di rischi specifici connessi allo svolgimento delle proprie mansioni e attività, di struttura e regolamento aziendale in materia di salute e sicurezza, procedure e misure di prevenzione e protezione e/o prendere atto dell'informazione fornita e/o partecipare attivamente ai corsi di formazione;

• utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i materiali, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;

• segnalare ai Responsabili o ai soggetti responsabili per la gestione della salute e sicurezza e/o all'OdV violazioni delle norme definite ed ogni situazione di pericolo potenziale o reale.

4.2.6. I reati di ricettazione, riciclaggio, auto-riciclaggio e impiego di beni di provenienza illecita ex art.25 octies D.lgs. n.231/01.

L'esposizione al rischio

La responsabilità amministrativa della Società ex D.lgs. n.231/01 può sorgere non solo per attività successive alla commissione di reati presupposto, in ordine ai quali sono stati conseguentemente già adottate specifiche misure di prevenzione, ma anche con riferimento ai rapporti finanziari con soggetti estranei alla compagine sociale, ed in particolare con i clienti ed i fornitori di STACK EMEA - ITALY .

A fronte del rischio nascente da condotte in qualche modo estranee all'operatività aziendale, emerge per altro verso l'importanza dei controlli effettuati sotto il profilo finanziario e contabile, oltre che in relazione alla congruità dei corrispettivi pattuiti ed all'effettività delle prestazioni "scambiate".

Principi generali di comportamento e regole di condotta

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla rubrica, ai Destinatari coinvolti nello svolgimento delle Attività Sensibili, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali, è fatto espresso divieto di porre in essere comportamenti:

• tali da integrare le fattispecie di reato sopra considerate;

• che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

• non in linea o non conformi con i principi e le prescrizioni contenute nel presente Modello e del Codice Etico o comunque con le procedure aziendali.

In particolare, i Destinatari dovranno:

• ispirarsi a criteri di trasparenza nell'esercizio dell'attività aziendale e nella scelta del partner finanziario e/o commerciale, prestando la massima attenzione alle notizie riguardanti i soggetti terzi con i quali STACK EMEA - ITALY ha rapporti di natura finanziaria o societaria, che possano anche solo generare il sospetto della commissione di uno dei reati di cui alla presente parte speciale;

• tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, con particolare riferimento alle attività finalizzate alla gestione anagrafica di Fornitori/clienti/Consulenti;

• non intrattenere in particolare rapporti commerciali con soggetti (persone fisiche e persone giuridiche) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità, quali, a titolo esemplificativo ma non esaustivo, soggetti legati o comunque riconducibili all'ambiente della criminalità organizzata, al riciclaggio, al traffico della droga, all'usura;

• conservare la documentazione a supporto, adottando tutte le misure di sicurezza, fisica e logica, instaurate da STACK EMEA - ITALY;

• mantenere un comportamento collaborativo con le Autorità di Vigilanza e/o giudiziarie;

• segnalare ai Responsabili di funzione eventuali violazioni delle norme e eventuali operazioni insolite che potrebbero essere un'indicazione per fenomeni di ricettazione, riciclaggio ed impiego di denaro, beni ed utilità di provenienza illecita, nonché autoriciclaggio;

• rispettare le procedure, direttive e policy aziendali applicabili in particolare alle attività svolte nell'ambito dei Processi Sensibili;

• osservare la massima attenzione in merito all'utilizzo dei proventi correlati ad operazioni economiche o a condotte di rilievo tributario che risultino oggetto di contestazione o che siano state comunque poste in discussione sotto il profilo della loro liceità e correttezza.

4.2.7. Reati ambientali ex art. 25-undecies D.Lgs.n.231/01

Coerentemente con il suo progetto imprenditoriale e con la richiamata aspirazione alla massima appetibilità ed efficienza dei servizi offerti, STACK EMEA – ITALY intende prestare assoluta attenzione alla sostenibilità ambientale, alla tutela dell'ambiente ed al risparmio energetico.

L'esposizione a rischio

In attesa dell'operatività societaria, le attività esposte al rischio di commissione dei reati in materia ambientale sono essenzialmente legate alla sola gestione delle sostanze chimiche (gasolio per i generatori) e dei rifiuti pericolosi e non pericolosi prodotti dal Data Center e dagli uffici di Assago. Inoltre, analogamente a quanto esposto in materia di prevenzione degli illeciti concernenti la sicurezza sul luogo di lavoro, STACK EMEA - ITALY ha interesse a che le aziende terze con le quali collabora per il raggiungimento dei propri scopi sociali, garantiscano di essere "*compliant*" in materia di norme ambientali.

Principi generali di comportamento

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla rubrica, i Destinatari coinvolti nello svolgimento delle Attività Sensibili nelle Aree a Rischio Reato individuate, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali ed istruzioni tecniche sono tenuti a:

- Rispettare le norme, gli obblighi e i principi posti dalla normativa vigente e dalla procedura interna di gestione degli aspetti ambientali;
- Rispettare i principi generali di condotta e comportamento ed i principi specifici formulati nel presente Modello;
- Promuovere il rispetto delle suddette norme, regole e principi al fine di assicurare gli adempimenti in materia di tutela ambientale;
- Adottare una condotta di massima collaborazione e trasparenza e rispettare le regole di condotta specificate nei rapporti con gli enti pubblici competenti in materia ambientale, sia in fase di stesura e comunicazione di eventuali dichiarazioni, sia in fase di richiesta ed ottenimento di autorizzazioni, sia in occasione di accertamenti e verifiche ispettive;
- Astenersi dall'abbandonare o depositare illegittimamente rifiuti sul suolo e nel suolo;
- Astenersi dall'immettere illegittimamente rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali o sotterranee;
- Astenersi dall'effettuare emissioni nocive nell'aria.

4.2.8. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare ex art. 25-duodecies.

Il rilascio del permesso di soggiorno concreta un vero e proprio effetto costitutivo della legittimazione dello straniero al lavoro, momento prima del quale non è per nulla possibile stipulare rapporti leciti (a pena di commissione del reato in oggetto). Viene dunque individuato nella pronta verifica della regolarità del soggiorno il bene giuridico tutelato dalla norma.

Il soggetto attivo del reato è il datore di lavoro. Tuttavia, la giurisprudenza assimila nel

concetto di datore di lavoro qualsiasi soggetto che “assuma alle proprie dipendenze, a tempo determinato o indeterminato, dietro la corresponsione di un compenso, una o più persone, aventi il compito di svolgere un'attività lavorativa subordinata di qualsiasi natura”.

Presupposto del reato è l’impiego alle proprie dipendenze di un cittadino straniero.

L’esposizione al rischio

Le attività nel cui ambito potrebbero astrattamente esser realizzata la fattispecie di reato richiamata dall’articoli 25-duodecies d.lgs. 231/2001 è rappresentata dalla gestione del processo di assunzione e gestione amministrativa del personale dipendente e di collaboratori extracomunitari. Le norme contenute in questa sezione e nei protocolli mirano ad eliminare la sussistenza di tale rischio.

Principi generali di condotta

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla rubrica, i Destinatari coinvolti nello svolgimento delle Attività Sensibili nelle Aree a Rischio Reato individuate, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali

- porre in essere condotte che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle di cui al presente paragrafo, possano potenzialmente diventarlo;
- porre in essere condotte non in linea o non conformi con i principi e le prescrizioni contenute nel presente Modello, nel Codice Etico
- In caso di assunzione di nuove risorse extracomunitarie, sarà necessario verificare i visti e/o permessi di soggiorno necessari per lo svolgimento della prestazione lavorativa.

4.2.9. I reati tributari ex art. 25 quinquiesdecies D.Lgs.n.231/01.

L’articolo 39 del decreto legge 26 ottobre 2019, n.124, come convertito e modificato dalla legge 19 dicembre 2019, n. 157, ha esteso la punibilità delle persone giuridiche

anche nel caso di reati tributari previsti dal D.lgs. 74/2000, commessi con “frode” e relativi ai documenti contabili o alla dichiarazione fiscale.

In particolare, con l’introduzione dell’art. 25-quinquiesdecies sono stati ricompresi nel catalogo dei reati presupposto il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (artt. 2), il delitto di dichiarazione fraudolenta mediante altri artifici (art. 3), il delitto di emissione di fatture o altri documenti per operazioni inesistenti (art. 8), il delitto di occultamento o distruzione di documenti contabili (art. 10), il delitto di sottrazione fraudolenta al pagamento di imposte (art. 11).

Inoltre, il decreto legislativo, 14 luglio 2020, n. 75 ha previsto la responsabilità degli enti alle ipotesi meno gravi previste dagli articoli 4 (dichiarazione infedele), 5 (omessa dichiarazione) e 10 quater (indebita compensazione) del. Dlgs 74/200, qualora tali delitti siano commessi “nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro”.

La possibile inerenza dei reati tributari ai molteplici processi aziendali che caratterizzano ogni società ha comportato, anche per STACK EMEA - ITALY , ed in attesa di una sua concreta operatività e di una più definita organizzazione, l’esigenza di implementare i presidi aziendali in modo da contenere adeguatamente il rischio reato nelle aree più esposte (Fiscalità e bilancio, Acquisizione di beni e servizi, Gestione Risorse finanziarie).

Principi generali di comportamento e regole di comportamento

Oltre ai principi generali già evidenziati nel codice etico e nelle procedure aziendali, ai destinatari del Modello è fatto assoluto divieto:

- di realizzare condotte tali da integrare le fattispecie di reato previste dall’art. 25-quinquiesdecies del Decreto;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa rendere difficilmente tracciabile l’operazione effettuata;

- di porre in essere attività che siano in contrasto con i principi generali di controllo finalizzati alla prevenzione dei reati tributari;

- di predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta e veritiera della realtà riguardo alla situazione economica, patrimoniale e finanziaria della società;

Inoltre, ai fini dell'attuazione dei comportamenti di cui sopra:

- nell'ambito dei rapporti con i consulenti, i fornitori, i partner commerciali e, in genere, con le controparti contrattuali deve essere garantito il rispetto del principio di correttezza trasparenza e buona fede;

- con riferimento alla attendibilità commerciale/professionale dei fornitori, devono essere richieste tutte le informazioni necessarie;

- gli incarichi conferiti ad eventuali aziende di servizi e/o persone fisiche che curino gli interessi economico-finanziari della Società devono essere anch'essi redatti per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite;

- è necessario che le funzioni competenti assicurino il controllo dell'avvenuta regolarità dei pagamenti nei confronti di tutte le controparti;

- la registrazione delle fatture passive avviene previa verifica dell'effettività della prestazione resa e della coerenza con la documentazione contrattuale, controllando l'inerenza della prestazione all'attività sociale;

- è necessario rispettare le regole e i principi contenuti nel Codice civile o altre normative e regolamenti vigenti in Italia e all'estero nonché i principi contabili italiani;

- è necessario assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;

- è necessario garantire la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte;

- qualora siano formulate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile, le stesse siano formalizzate, motivate e ne sia fornita adeguata informazione alle Funzioni/Organi competenti;

- chi fornisce informazioni alle unità gerarchicamente sovraordinate è tenuto a indicare i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, al fine di garantire la verificabilità delle stesse.

In particolare, l'attività di approvvigionamento di beni, lavori e servizi deve prevedere:

- la pianificazione annuale degli acquisti;

- per ogni acquisto, la definizione del fabbisogno e dei requisiti minimi in possesso dei soggetti offerenti;

- la definizione dei criteri per la determinazione dei compensi da corrispondere al fornitore;

- la predisposizione e autorizzazione delle richieste/proposte di acquisto;

- la verifica del possesso da parte del fornitore dei requisiti professionali e reputazionali;

- la definizione dei ruoli, compiti e responsabilità connessi alla gestione dell'anagrafica fornitori (es. ruoli aziendali responsabili di richiedere la creazione/modifica di fornitori in anagrafica, le modalità con le quali tali richieste devono essere inoltrate, le attività di controllo da svolgere a seguito dell'avvenuta modifica dell'anagrafica fornitori);

- che il soggetto che autorizza l'ordine di acquisto sia munito a tal fine di appositi poteri;

- la trasparenza nella valutazione delle offerte (tecniche/economiche);

- l’effettiva verifica circa la corretta esecuzione dei lavori o servizi, l’avvenuta consegna dei lavori, del bene o erogazione del servizio rispetto ai requisiti e ai termini definiti negli ordini/contratti.

4.2.10. Reati di contrabbando (art. 25-sexiesdecies).

Il decreto legislativo, 14 luglio 2020, n. 75, ha esteso la responsabilità degli enti ai reati di contrabbando previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, facendo un generico richiamo ai “reati” ivi previsti. Peraltro, mentre il D.lgs. 8/2016 aveva depenalizzato (anche) gli illeciti doganali puniti sono con la multa o solo con l’ammenda, il nuovo d.lgs. 75/2020 ha comportato la reviviscenza di tali reati, qualora l'ammontare dei diritti di confine dovuti sia superiore a diecimila euro.

Ne consegue che, ad oggi, sono reati presupposto della responsabilità degli enti i reati di contrabbando sia i delitti puniti con la pena detentiva (articolo 291-bis, Contrabbando di tabacchi lavorati esteri, articolo 291-quater, Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri, e articolo 295, Contrabbando aggravato) che i reati puniti con la sola pena pecuniaria, qualora in quest’ultimo caso i diritti di confine siano superiori a 10.000 euro. Si rinvia sul punto all’allegato elenco dei reati presupposto.

L’esposizione al rischio

L’introduzione dei delitti di contrabbando all’interno dei reati presupposto comporta un parziale aumento del rischio nei confronti della Società, seppur remoto a fronte dell’attività sociale svolta da STACK EMEA - ITALY . In particolare, il rischio concerne l’approvvigionamento di beni acquisiti in violazione del Testo Unico Doganale, con il possibile concorso di soggetti interni alla struttura societaria.

Principi generali di condotta

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla rubrica, i Destinatari coinvolti nello svolgimento delle Attività Sensibili nelle Aree a Rischio Reato individuate sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali:

- è vietato porre in essere condotte che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle di cui al presente paragrafo, possano potenzialmente diventarlo;
- è vietato porre in essere condotte non in linea o non conformi con i principi e le prescrizioni contenute nel presente Modello e nel Codice Etico;
- i Destinatari devono assicurare il rispetto del Protocollo 231 Approvvigionamenti Beni e Servizi;
- Nel caso di acquisti di beni soggetti a dazi doganali, è obbligatorio verificarne il rispetto del pagamento dei diritti di confini, segnalando immediatamente all'ODV ogni anomalia.

Gli altri reati

Si precisa che il preliminare esame e assessment del complesso delle attività aziendali ha condotto a ragionevolmente escludere la possibilità di commissione di alcuni reati presupposto, sia in ragione delle caratteristiche della società (ad es. False comunicazioni sociali delle società quotate ex art. 2622 c.c.), sia in ragione della circostanza che alcuni di essi non possono essere consumati nell'interesse/vantaggio di STACK EMEA - ITALY (ad es. detenzione di materiale pornografico), sia perché l'eventualità della loro consumazione è altamente improbabile e la loro configurazione è meramente scolastica.

Sono stati esclusi: i Reati contro la personalità individuale (tra cui il Caporalato) ex Art. 25-quinquies D.lgs. 231/2001, i Delitti contro l'industria e il commercio ex art.25 bis-1 D.Lgs. n.231/01, i reati di falso nummario, i reati contro la personalità individuale in materia di pornografia e prostituzione minorile, mutilazione dei genitali femminili, i delitti con finalità di terrorismo o di eversione dell'ordine democratico, i c.d. di *market abuse* (abuso di informazioni privilegiate e manipolazione del mercato), i reati di scambio elettorale politico-mafioso e di sequestro di persona a scopo di rapina o estorsione; i reati di associazione finalizzata al traffico di sostanze stupefacenti o psicotrope; i delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o

tipo guerra o parti di esse, di esplosivi, di armi clandestine, nonché di più armi comuni da sparo, il reato di Razzismo e Xenofobia ex art. 25-terdecies, i reati di Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati *ex* art. 25-quaterdecies. In relazione a tali fattispecie di reato, ad ogni modo, troveranno, per quanto possibile, applicazione le disposizioni del Codice Etico e i presidi facenti parte del Sistema di Gestione Integrato e dei controlli interni.

Analogamente, ai fini della prevenzione del reato di induzione a non rendere dichiarazioni ovvero a rendere dichiarazioni mendaci nei confronti dell'Autorità Giudiziaria, varranno i principi ed i presidi contenuti nel Codice Etico e nelle procedure aziendali richiamate.

****

5. L'Organismo di Vigilanza e Controllo

5.1. Generalità

Come già anticipato, il decreto legislativo prevede, all'art. 6, comma 1, lett. b) che l'Ente non risponde per gli eventuali reati commessi al suo interno se il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione e gestione predisposto, nonché di curarne l'aggiornamento, sia stato affidato ad un Organismo (OdV) dell'Ente dotato di autonomi poteri di iniziativa e controllo.

La compiuta esecuzione dei propri compiti da parte dell'OdV costituisce elemento essenziale per l'esimente prevista dal Decreto.

5.2. Nomina e composizione

In considerazione della ridotta complessità organizzativa emergente dall'attuale contesto societario, STACK EMEA - ITALY si avvale di un OdV a composizione monocratica. Il soggetto chiamato a rivestire la relativa carica è scelto tra professionisti qualificati, quali in particolare avvocati o dottori commercialisti, in possesso dei necessari

requisiti di onorabilità da intendersi così come richiamati dall'art.4, Decreto 30 dicembre 1998, n.516 che non si trovino in conflitto di interessi.

Il componente dell'OdV è nominato dall'organo amministrativo con comunicazione formale nella quale vengono indicati, la durata dell'incarico ed il compenso.

La nomina è comunicata tempestivamente mediante adeguati mezzi di comunicazione.

5.3. Durata in carica, sostituzione e revoca dell'OdV

Ogni componente dell'OdV resta in carica per il tempo indicato nel mandato, non inferiore ai tre anni, eventualmente rinnovato per uguale periodo e comunque sino alla nomina del nuovo successore.

Nel caso in cui il componente dell'OdV incorra in una delle cause di incompatibilità di cui ai successivi paragrafi, l'organo amministrativo previa raccolta degli elementi a comprova del fatto e sentito l'interessato, stabilisce un termine, non inferiore a 30 giorni entro il quale deve essere cessata la situazione di incompatibilità. Trascorso tale termine senza che l'incompatibilità sia cessata, l'organo amministrativo deve revocare il mandato.

Il mandato sarà altresì revocato:

- qualora sussistano circostanze tali da far venire meno i requisiti di autonomia ed indipendenza richiesti dalla legge;
- qualora il componente sia soggetto ad una sentenza di condanna, ancorché non definitiva, per uno dei reati previsti dal Decreto, ovvero che importi l'interdizione, anche temporanea dai pubblici uffici o incapacità di esercitare uffici direttivi;
- qualora vengano meno i requisiti di onorabilità di cui ai paragrafi successivi.

È facoltà del componente dell'OdV rinunciare in qualsiasi momento all'incarico. In tal caso, egli deve darne formale comunicazione all'organo amministrativo motivando le ragioni che hanno determinato la rinuncia.

La revoca dell'incarico potrà essere eseguita solo per giusta causa.

A tale riguardo, per giusta causa di revoca dovrà intendersi:

- interdizione o l'inabilitazione, ovvero, una grave infermità che renda il componente dell'OdV non idoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti l'impossibilità a compiere il proprio lavoro per un periodo superiore ai sei mesi;
- un grave inadempimento dei propri doveri così come definiti nel presente modello;
- una grave negligenza nell'espletamento dei compiti connessi all'incarico;
- una sentenza di condanna della Società ai sensi del Decreto passata in giudicato, ovvero un procedimento penale concluso tramite il c.d. "patteggiamento", ove risulti dagli atti "l'omessa o insufficiente vigilanza da parte dell'OdV, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- una sentenza di condanna, ancorché non definitiva, per uno dei reati previsti dal Decreto, ovvero che importi l'interdizione, anche temporanea dai pubblici uffici o incapacità di esercitare uffici direttivi.

Nei casi sopra descritti l'organo amministrativo provvederà a nominare il nuovo componente dell'OdV.

5.4. I requisiti dell'Organismo di Vigilanza e Controllo

Autonomia e indipendenza

STACK EMEA - ITALY si impegna a garantire all'OdV piena autonomia di iniziativa ed a preservarlo da qualsiasi forma di interferenza o di condizionamento. A tale fine è previsto che:

- I suoi componenti non abbiano compiti operativi e non abbiano possibilità di ingerenza nell'operatività della Società;
- l'Organismo nello svolgimento della propria funzione non sia soggetto a potere gerarchico e disciplinare di alcun organo o funzione societaria;
- riporti direttamente all'organo amministrativo;

- l'adozione delle sue decisioni inerenti alle attività di verifica e di controllo ritenute necessarie siano insindacabili.

Professionalità

Per assicurare il corretto svolgimento dei propri compiti, è essenziale che l'Organismo garantisca una adeguata professionalità. Sotto tale aspetto assume rilevanza:

- la conoscenza di materie giuridiche (in particolare della struttura e delle modalità di commissione dei reati presupposto, nonché del Decreto nel suo complesso);
- la conoscenza della struttura organizzativa della Società;
- un'adeguata competenza in materia di auditing e controllo.

Onorabilità e assenza di conflitto di interessi

Tale requisito va inteso nei seguenti termini:

- i componenti dell'OdV sono scelti tra soggetti qualificati e dotati di spiccata professionalità ed in possesso dei requisiti di onorabilità da intendersi così come richiamati dall'art.4, Decreto 30 Dicembre 1998, n.516.
- i componenti dell'OdV non devono avere vincoli di parentela con il vertice aziendale e devono essere liberi da qualsiasi situazione che possa generare in concreto conflitto di interessi.

Continuità d'azione

La continuità di azione dell'OdV viene garantita dalla professionalità del medesimo, dalla durata minima della relativa carica e dalla possibilità di revoca solo per giusta causa nei termini sopra descritti.

5.5. Le risorse dell'Organismo di Vigilanza

L'organo amministrativo assegna all'OdV le risorse umane e finanziarie ritenute opportune al fine dello svolgimento dell'incarico, comunque adeguate alle dimensioni della Società e ai compiti spettanti all'OdV in funzione del grado di esposizione al rischio. Con riguardo alle risorse finanziarie, l'Organismo potrà disporre del budget assegnatogli annualmente anche su proposta dell'Organismo stesso.

Per quanto attiene alle risorse umane l'OdV potrà avvalersi del personale assegnatogli, di consulenti esterni e dell'ausilio di tutte le strutture della Società.

In caso di necessità, l'OdV potrà richiedere all'organo amministrativo, mediante comunicazione scritta e motivata, l'assegnazione di ulteriori risorse umane o finanziarie.

Con precipuo riferimento alle questioni connesse alla tutela della salute e sicurezza sul lavoro (D.Lgs. n.81/08) l'OdV potrà avvalersi di tutte le risorse disponibili per la gestione dei relativi aspetti. L'Odv, nelle relazioni di propria competenza, rendiconterà l'utilizzo del budget assegnatogli.

5.6. Convocazione

L'OdV si riunisce ogni volta che sia ritenuto opportuno dal suo componente e comunque almeno due volte l'anno. Di ogni riunione viene redatto specifico verbale.

Ove possibile, la documentazione cartacea di pertinenza dell'OdV ed i verbali delle sue riunioni, sono custoditi in azienda, in uno spazio dedicato e riservato ed al quale può accedere solo l'OdV stesso.

5.7. Obbligo di riservatezza

L'OdV è tenuto al segreto in ordine alle notizie ed informazioni acquisite nell'esercizio delle loro funzioni. Il componente dell'OdV assicura la riservatezza delle informazioni di cui venga in possesso, in particolare se relative alle segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello. In ogni caso, ogni informazione in possesso dell'OdV viene trattata in conformità con la legislazione vigente in materia, nel rispetto della procedura di *whistleblowing* di seguito descritta.

5.8. Compiti e poteri dell'Organismo di Vigilanza

In conformità a quanto previsto dall'art. 6, comma 1 del Decreto, che gli affida il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento, all'OdV della Società, fanno capo i seguenti compiti:

- verificare l'adeguatezza del Modello ovvero la sua idoneità astratta a prevenire il verificarsi di comportamenti illeciti;
- vigilare sul funzionamento e sull'osservanza del modello:

- programmando l'attività di verifica ispettiva, e riesaminando i risultati delle verifiche ispettive precedenti,
- effettuando verifiche sulle attività od operazioni individuate nelle aree a rischio (es. aggiornamento delle procedure, sistema di deleghe in termine di coerenza tra poteri conferiti ed attività espletate, conoscenza del Modello),
- incontrando le strutture di vertice di STACK EMEA - ITALY, al fine di confrontarsi, verificare e relazionare sull'andamento del modello di organizzazione e gestione,
- promuovendo incontri con l'organo amministrativo, ogni volta che ritenga opportuno un esame o un intervento per discutere in materie inerenti il funzionamento e l'efficacia del modello di organizzazione e gestione;

- verificare l'effettività del modello, ovvero la corrispondenza tra i comportamenti concreti e quelli formalmente previsti dal Modello stesso;
- predisporre, modificare o meglio specificare il sistema di comunicazione interna al fine di al fine di poter ricevere le segnalazioni di possibili violazioni e/o inosservanze del modello
- eseguire o verificare che venga svolta un'idonea attività di formazione ed informazione rivolta ai dipendenti e collaboratori della Società, in particolare promuovendo e definendo le iniziative per la diffusione della conoscenza circa il decreto e le conseguenze derivanti dalla sua applicazione;
- verificare che il modello sia aggiornato ed attivarsi per il suo aggiornamento, qualora ritenuto necessario (ad es. a seguito di modifiche organizzative/gestionali, di adeguamenti legislativi delle norme cogenti, di acclarate violazioni al modello e/o al codice etico);
- garantire un flusso di informazioni verso il vertice societario.

Da precisare che, quanto alla cura dell'aggiornamento del modello, l'adozione di eventuali modifiche dello stesso è di competenza dell'organo amministrativo, il quale ha la responsabilità diretta dell'adozione e dell'efficace attuazione del modello stesso.

La funzione di vigilanza è estesa anche al Codice Etico sul quale l'Organismo di Vigilanza svolge l'attività di monitoraggio.

Nell'esecuzione dei suoi compiti, l'OdV è sempre tenuto a:

- documentare, anche mediante la compilazione e la tenuta di appositi registri, tutte le attività svolte ed i provvedimenti adottati;
- documentare le segnalazioni e le informazioni ricevute, al fine di garantire la tracciabilità degli interventi;
- registrare e conservare tutta la documentazione.

Per l'espletamento dei compiti ad esso assegnati, all'Organismo sono riconosciuti tutti i poteri necessari ad assicurare una puntuale ed efficiente vigilanza, in particolare:

- effettuare, anche senza avviso, tutte le verifiche ispettive ritenute opportune;
- accedere liberamente presso le aree di tutte le funzioni, gli archivi ed i documenti della Società;
- avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture della Società o di consulenti esterni;
- disporre direttamente delle risorse finanziarie appositamente stanziate.

5.9. Gestione delle verifiche del sistema di controllo interno

L'OdV disciplinerà nel proprio regolamento di funzionamento la periodicità e le modalità con le quali svolgerà l'attività di verifica ispettiva, ordinaria ed eventualmente straordinaria, sul sistema di controllo interno della società così come descritto al punto 4. del presente documento e, più precisamente, sulla corretta osservanza e sul rispetto dei principi generali e particolari (protocolli 231) disciplinati dal Modello.

5.10. Flusso di informazione verso l'Organismo di Vigilanza

Ai sensi dell'art. 6, comma 2, lett. d) del decreto, viene istituito l'obbligo di informazione verso l'OdV in merito a situazioni di potenziale rischio di illecito, o ad atti che si configurino come violazioni del Sistema.

Segnalazione

Il personale dipendente (ovvero collaboratore esterno) della Società che intenda segnalare una violazione (o presunta violazione) del modello è tenuto a contattare l'OdV attraverso apposita casella e-mail dedicata (*organismodivigilanza-italy@stackinfra.com*) oppure tramite comunicazione scritta, ovvero sulla PEC professionale del soggetto chiamato a svolgere la funzione di Organismo di vigilanza, come pubblicata sui relativi albi professionali. Nel caso di segnalazioni anonime e non in forma scritta, l'OdV le valuterà a sua discrezione a seconda della gravità della violazione denunciata.

L'Organismo agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione o penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa la loro identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti di STACK EMEA - ITALY o delle persone accusate erroneamente e/o in mala fede.

Attivazione dell'OdV

L'OdV esamina tutte le segnalazioni pervenute alla propria attenzione, le valuta e, in caso lo ritenga necessario, si attiva avviando tutte le indagini ritenute necessarie, quali ad esempio:

- la convocazione del responsabile della violazione (o presunta tale);
- il coinvolgimento delle funzioni interessate dalla segnalazione;
- l'accesso a qualunque fonte di informazione della Società, documento o dato ritenuto rilevante ai fini dell'inchiesta.

Altre informazioni

È fatto obbligo a tutta l'Organizzazione (Organi societari, Dirigenti, responsabili e dipendenti) di comunicare all'OdV le informazioni riportate nella tabella successiva; in particolare, la frequenza di segnalazione è distinta in:

- A evento: ogni qual volta si verifichi l'episodio, senza indebiti ritardi;

- Riunione dell'OdV: l'Organismo comunica con adeguato anticipo alle funzioni aziendali la prossimità della propria riunione, così da poter consentire alle stesse la predisposizione del flusso informativo specificato;
- Frequenza specifica, valutata sulla base della potenziale criticità e dei volumi legati all'informativa.

Reporting periodico

Con cadenza annuale, l'Organo Amministrativo (o il soggetto formalmente delegato) trasmette all'ODV i seguenti documenti:

- Elenco dipendenti assunti/cessati nell'anno ed eventuali anomalie;

- Elenco premi/bonus/benefit assegnati;

- Elenco dei Fornitori che hanno ricevuto importi superiori a 30.000 euro ed eventuale documentazione contrattuale di riferimento;

- Elenco di consulenti che hanno avuto incarichi professionali con affidamento diretto per importi superiori a 10.000 euro;

- Elenco fornitori con valutazione negativa a seguito di gravi criticità riscontrate;

- Disallineamenti degli importi tra fatture in pagamento e contratti;

- Contratti con criticità (contratti con scostamenti significativi dai prezzi normali o dal listino standard, contratti per i quali pende un contenzioso, emersione di anomalie reputazionali delle controparti);

- Piano della Formazione in materia di sicurezza sul lavoro;

- Adozione e/o modifiche del DVR;

- Accordi stipulati con società collegate;

- Fascicolo di bilancio;

- Dichiarazioni tributarie annuali;

- Elenco fatture attive e passive;

- Elenco degli avvisi di verifica e/o richieste inoltrate da Pubblici Ufficiali o incaricati di pubblico servizio;

- Elenco contratti/appalti in corso con PP.AA., con indicazione di eventuali criticità;

- Elenco degli omaggi, delle sponsorizzazioni e delle liberalità, effettuati e ricevuti, con indicazione degli importi, dei motivi dell'atto e dei beneficiari.

5.11. Reporting e gestione dei documenti

Al fine di garantire la sua piena autonomia e indipendenza, l'OdV riporta direttamente all'organo amministrativo.

In sede di approvazione del bilancio l'OdV riferisce, mediante relazione scritta, circa lo stato di attuazione del modello, circa i seguenti elementi:

- l'attività di vigilanza svolta dall'Organismo nel periodo di riferimento;
- le eventuali criticità emerse sia in termini di comportamenti interni sia in termini di efficacia dei Modello;
- gli interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione.

L'OdV potrà essere convocato in ogni momento dall'organo amministrativo per riferire su particolari eventi o situazioni relative all'efficacia ed all'efficienza del Modello; potrà altresì in ogni momento chiedere di essere sentito qualora ritenga opportuno un esame o un intervento del suddetto organo circa l'adeguatezza del Modello.

L'Organismo di Vigilanza ha l'obbligo di informare immediatamente il legale rappresentante qualora la violazione del modello riguardi gli apicali dell'Azienda, nonché l'Assemblea dei soci qualora la violazione riguardi il legale rappresentante.

Gli incontri con i soggetti ed organi sopra indicati devono essere verbalizzati e copie dei verbali saranno custodite dall'Organismo.

.

****

6. Il sistema disciplinare

6.1. Finalità del sistema disciplinare

STACK EMEA - ITALY considera essenziale il rispetto del Codice Etico e del Modello e, pertanto, in ottemperanza agli artt. 6, co. 2, lett. e), e 7, co. 4, lett. b) del D.Lgs.231/01, ha adottato un adeguato sistema sanzionatorio da applicarsi in caso di mancato rispetto delle norme previste dal Modello stesso, poiché la violazione di tali norme e misure lede il rapporto di fiducia instaurato con la Società.

Ai fini dell'applicazione delle sanzioni disciplinari ivi previste, l'instaurazione di eventuali procedimenti penali e il loro esito non sono necessari, poiché le norme e le misure previste nel Modello sono adottate da STACK EMEA - ITALY in piena autonomia, a prescindere dal reato che eventuali condotte possano determinare.

In nessun caso una condotta illecita, illegittima o comunque in violazione del Modello potrà essere giustificata o ritenuta meno grave, anche se compiuta nell'interesse o a vantaggio di STACK EMEA - ITALY . Sono altresì sanzionati i tentativi e, in particolare, gli atti od omissioni in modo non equivoco diretti a violare le norme e le regole stabilite dalla Società, anche se l'azione non si compie o l'evento non si verifica per qualsivoglia motivo.

6.2. Sanzioni per i lavoratori dipendenti subordinati

In conformità alla legislazione applicabile, STACK EMEA - ITALY deve informare i propri dipendenti delle disposizioni, principi e regole contenuti nel Modello di Organizzazione, Gestione e Controllo, mediante le attività di informazione e formazione descritte nel capitolo seguente.

La violazione da parte del dipendente delle disposizioni, principi e regole contenuti nel Modello predisposto da STACK EMEA - ITALY al fine di prevenire la commissione di reati ai sensi del Decreto 231 costituisce un illecito disciplinare, punibile secondo le procedure di contestazione delle violazioni e l'irrogazione delle conseguenti sanzioni previste nella sezione "Norme Disciplinari" e conformi alla normativa vigente.

Il sistema disciplinare relativo al Modello è stato configurato nel puntuale rispetto di tutte le disposizioni di legge in materia di lavoro. Non sono state previste modalità e sanzioni diverse da quelle già codificate e riportate nei contratti collettivi e negli accordi sindacali.

A titolo esemplificativo e non esaustivo, costituisce illecito disciplinare, relativamente alle attività individuate a rischio di reato:

- la mancata osservanza dei principi contenuti nel Codice Etico e di Comportamento o l'adozione di comportamenti comunque non conformi alle regole del Codice Etico e di Comportamento;
- il mancato rispetto delle norme, regole e procedure di cui al Modello;
- la mancata, incompleta o non veritiera documentazione o la non idonea conservazione della stessa necessarie per assicurare la trasparenza e verificabilità dell'attività svolta in conformità alle norme procedure di cui al Modello;
- la violazione e l'elusione del sistema di controllo, realizzate mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dalle procedure di cui sopra;
- l'ostacolo ai controlli e/o l'impedimento ingiustificato all'accesso alle informazioni ed alla documentazione opposto ai soggetti preposti ai controlli stessi, incluso l'Organismo di Vigilanza.

Le suddette infrazioni disciplinari possono essere punite, a seconda della gravità delle mancanze, con i seguenti provvedimenti:

- ammonizione verbale;
- ammonizione scritta;
- multa
- sospensione
- licenziamento.

Le sanzioni devono essere comminate avuto riguardo della gravità delle infrazioni: in considerazione dell'estrema importanza dei principi di trasparenza e tracciabilità, nonché

della rilevanza delle attività di monitoraggio e controllo, la Società sarà portata ad applicare i provvedimenti di maggiore impatto nei confronti di quelle infrazioni che per loro stessa natura infrangono i principi stessi su cui si fonda il presente Modello.

Il tipo e l'entità di ciascuna delle sanzioni devono essere applicate tenendo conto:

- dell'intenzionalità del comportamento o del grado di negligenza, imprudenza od imperizia con riguardo anche alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti di legge;
- delle mansioni del lavoratore;
- della posizione funzionale e del livello di responsabilità e autonomia delle persone coinvolte nei fatti costituenti la mancanza;
- delle altre particolari circostanze relative all'illecito disciplinare.

6.3. Sanzioni nei confronti del personale dirigente

In caso di violazione del Modello da parte di dirigenti l'Organismo di Vigilanza dovrà informare l'Organo Amministrativo.

La Società provvederà ad irrogare le misure disciplinari più idonee. Peraltro, alla luce del più profondo vincolo fiduciario che, per sua stessa natura, lega la Società al personale dirigente, nonché in considerazione della maggiore esperienza di questi ultimi, le violazioni alle disposizioni del Modello in cui i dirigenti dovessero incorrere comporteranno soprattutto provvedimenti espulsivi, in quanto considerati maggiormente adeguati.

6.4. Misure nei confronti dei membri del CdA

Alla notizia di violazione dei principi, delle disposizioni e delle regole di cui al presente Modello da parte dei membri del CdA, l'Organismo di Vigilanza è tenuto ad informare l'assemblea dei soci.

6.5. Misure nei confronti di altri destinatari

Il rispetto da parte di coloro che, a qualsiasi titolo, operano in nome e per conto di STACK EMEA - ITALY e da parte degli altri destinatari delle norme del Codice Etico e di Comportamento e del Modello, è garantito da specifiche clausole contrattuali aventi ad oggetto le sanzioni applicabili in caso di inosservanza del Codice Etico e del Modello. Ogni violazione, o l'eventuale commissione da parte di tali soggetti dei reati previsti dal Decreto 231 sarà non solo sanzionata secondo quanto previsto nei contratti stipulati con gli stessi, ma anche attraverso le opportune azioni giudiziali di tutela della Società.

6.6. Ulteriori misure

Resta salva la facoltà di STACK EMEA - ITALY di avvalersi di tutti gli altri rimedi consentiti dalla legge, ivi inclusa la possibilità di richiedere il risarcimento dei danni derivanti dalla violazione del Decreto 231 da parte di tutti i soggetti sopra elencati.

****

7. Formazione e informazione

7.1. Formazione del personale

Ai fini dell'efficacia del presente Modello, è obiettivo di STACK EMEA - ITALY garantire una corretta divulgazione e conoscenza delle regole di condotta ivi contenute nei confronti delle risorse già presenti in azienda e di quelle da inserire, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle attività a rischio.

Il sistema di informazione e formazione è supervisionato dall'Organismo di Vigilanza, in collaborazione con i responsabili delle Funzioni o Aree aziendali di volta in volta coinvolte nell'applicazione del Modello.

La comunicazione iniziale

Il presente Modello è comunicato ai nuovi assunti ed a tutte le risorse presenti in azienda al momento dell'adozione dello stesso mediante adeguate forme di comunicazione.

La formazione

L'attività di formazione, finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001, è differenziata nei contenuti e nelle modalità di erogazione in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società.

7.2. Informativa a collaboratori ed altri soggetti terzi

I collaboratori e le terze parti contraenti che operano, a qualunque titolo, per conto o nell'interesse di STACK EMEA - ITALY e che sono coinvolti nello svolgimento di attività "sensibili" ai sensi del Decreto, devono essere informati, per le parti di rispettivo interesse, del contenuto del Modello e dell'esigenza di STACK EMEA - ITALY che il loro comportamento sia conforme ai disposti del D.lgs. n.231/2001.

****

8. Whistleblowing

8.1 Premessa

Per "whistleblowing" (di seguito "**Segnalazione**") si intende qualsiasi notizia riguardante condotte sospette non conformi a quanto stabilito dal Codice Etico, dal Modello adottato dalla Società e dal D.lgs. 231/2001, nonché dalle procedure interne e dalla disciplina esterna comunque applicabile a STACK EMEA - ITALY . Nessuna conseguenza negativa deriva in capo a chi abbia in buona fede effettuato una Segnalazione ed è assicurata la riservatezza dell'identità del segnalante.

8.2 Contesto normativo

Con la legge 30 novembre 2017, n. 179 è stata introdotta nell'ordinamento la disciplina in materia di *whistleblowing*, ovvero le "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".

Tale legge ha altresì innovato il testo del D.lgs. 231/2001 laddove, introducendo i commi 2 bis, 2 ter e 2 quater nell'articolo 6 del D.lgs. 231/2001, ha disposto che i modelli di organizzazione e gestione devono prevedere: i) a carico dei vertici aziendali, dipendenti o collaboratori, l'obbligo di presentare, in buona fede, segnalazioni circostanziate di

condotte illecite, rilevanti ai sensi del D.lgs. 231/2001 o violazioni del Modello di cui siano venuti a conoscenza in ragione delle funzioni svolte; ii) canali alternativi di segnalazione, nonché misure volte a garantire la riservatezza circa l'identità del segnalante; iii) il divieto di atti ritorsivi o discriminatori nei confronti del *whistleblower* per motivi legati alla segnalazione; iv) l'inserimento, all'interno del sistema disciplinare, di sanzioni nei confronti di chi violi gli obblighi di riservatezza o compia atti di ritorsione nei confronti del denunciante; v) la possibilità, per il segnalante o il relativo sindacato, di denunciare all'Ispettorato del Lavoro eventuali misure discriminatorie adottate dalla società nei suoi confronti, nonché chiedere la nullità del licenziamento/demansionamento ritorsivo o discriminatorio del *whistleblower*.

8.3 Destinatari

Destinatari della presente procedura sono:

- i vertici aziendali di STACK EMEA - ITALY;
- tutti i dipendenti di STACK EMEA - ITALY;
- i partner, i clienti, i fornitori, i consulenti, i collaboratori, i soci e, più in generale, chiunque sia in relazione d'interessi con la Società ("**Terzi**").

8.4 Scopo della procedura di Whistleblowing

Il presente documento (di seguito "**Procedura di Whistleblowing**") si propone di disciplinare il processo di ricezione, analisi e trattamento delle Segnalazioni, da chiunque inviate o trasmesse. Tali Segnalazioni riguardano, in particolare, i seguenti ambiti inerenti al sistema di controllo:

a) richieste di chiarimenti sulla correttezza di comportamenti propri o altrui ai fini della piena osservanza del Codice Etico, del Modello e del D.lgs. 231/2001 in generale (es: violazione di divieti e disposizioni aziendali, controlli sull'operato dei fornitori);

b) comunicazioni di presunte violazioni, di richieste o di induzioni alla violazione di norme di legge o regolamento, di prescrizioni del Codice Etico del Modello e del D.lgs. 231/2001 in generale, di procedure interne, con riferimento alle attività e prestazioni di interesse

della Società (es: inosservanza di clausole contrattuali, diffamazione, minacce, violazione della privacy, frodi, improprio utilizzo di dotazioni aziendali);

c) comunicazioni di presunte violazioni del Modello e del D.lgs. 231/2001 in generale anche a seguito di comportamenti a rischio reato e/o illecito previsti dal Modello e del D.lgs. 231/2001 in generale;

d) denunce, provenienti da Terzi aventi ad oggetto presunti rilievi, irregolarità e fatti censurabili;

e) esposti riguardanti tematiche di contabilità e controlli.

8.5 Invio delle segnalazioni

I Destinatari inviano le Segnalazioni secondo le modalità di seguito esposte, non appena vengano a conoscenza degli eventi che le hanno generate. Qualora un dipendente dovesse ricevere una Segnalazione da altri soggetti (ad es. altri dipendenti/Terzi), lo stesso ha l'obbligo di trasmettere la Segnalazione medesima, con immediatezza ed in via esclusiva, sempre secondo le modalità di seguito esposte, completa di tutta la eventuale documentazione di supporto pervenuta, non trattenendone copia ed astenendosi dall'intraprendere alcuna iniziativa autonoma di analisi e/o approfondimento. La mancata comunicazione di una Segnalazione ricevuta costituisce una violazione della presente Procedura di Whistleblowing, con l'applicazione, in caso di accertata malafede di tali condotte, delle conseguenti sanzioni disciplinari di cui al presente Modello.

La segnalazione deve essere inviata esclusivamente all'Organismo di Vigilanza mediante qualunque supporto scritto (posta ordinaria, e-mail, fax, sms) ovvero attraverso un indirizzo di posta elettronica appositamente ed esclusivamente dedicato dalla Società alla ricezione delle Segnalazioni da parte dell'Organismo di Vigilanza medesimo. Tale sistema dedicato, inoltre, consentirà di tenere riservata, in prima battuta e salva in ogni caso la possibilità di una successiva indagine, l'identità del segnalante, il cui indirizzo di posta elettronica dal quale sia partita la Segnalazione arriverà all'indirizzo di posta elettronica dedicato in forma criptata. Al fine di garantire la riservatezza, il segnalante potrà inoltre

inviare la segnalazione sulla PEC del professionista chiamato a svolgere la funzione di Organismo di vigilanza, come pubblicata sui relativi albi professionali.

L'Organismo di Vigilanza, all'atto della ricezione di una Segnalazione, provvederà a conservare la medesima, garantendone la riservatezza. L'organismo archivierà altresì tutta la documentazione e le e-mail scambiate inerenti a ciascuna Segnalazione, sino alla chiusura della stessa.

Tutte le Segnalazioni sono oggetto di analisi preliminare da parte dell'Organismo di Vigilanza al fine di verificare la presenza di dati ed informazioni utili a consentire una prima valutazione della fondatezza della Segnalazione stessa.

Qualora a conclusione della fase di analisi preliminare emerga l'assenza di elementi sufficientemente circostanziati o, comunque, l'infondatezza dei fatti richiamati nella Segnalazione, quest'ultima sarà archiviata dall'Organismo di Vigilanza, con le relative motivazioni.

Con riferimento a ciascuna Segnalazione, laddove, a seguito delle analisi preliminari, emergano o siano comunque desumibili elementi utili e sufficienti per una valutazione della fondatezza della Segnalazione medesima, fatto salvo il diritto alla difesa del segnalato, l'Organismo di Vigilanza provvederà a:

a) avviare analisi specifiche (eventualmente anche tramite attività di audit) nonché coinvolgendo le funzioni aziendali interessate dalla Segnalazione e in ogni caso informando l'Organo Amministrativo;

b) concludere l'istruttoria in qualunque momento, se, nel corso dell'istruttoria medesima, sia accertata l'infondatezza della Segnalazione;

c) avvalersi, se necessario, di esperti o periti esterni alla Società;

d) informare l'Organo Amministrativo affinché questi valuti l'eventuale "*action plan*" necessario per la rimozione delle debolezze di controllo rilevate, garantendo altresì il monitoraggio dell'attuazione;

e) informare l'Organo Amministrativo, affinché siano valutate eventuali iniziative da intraprendere prima della chiusura della Segnalazione stessa;

f) informare l'Organo Amministrativo affinché questi valuti eventuali iniziative da intraprendere a tutela degli interessi della Società (ad es. azioni giudiziarie, sospensione/cancellazione dei contratti in essere con la Società);

g) informare l'Organo Amministrativo affinché questi valuti l'avvio di un procedimento disciplinare nei confronti del segnalante, anche ai sensi di quanto previsto nella Sezione 4 del presente Modello, nel caso di Segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa Segnalazione;

h) sottoporre alla valutazione dell'Organo Amministrativo gli esiti degli approfondimenti della Segnalazione, qualora si riferisca a dipendenti e risulti fondata, affinché vengano intrapresi i più opportuni provvedimenti verso i dipendenti segnalati;

i) informare in ogni caso l'Organo Amministrativo in merito a tutte le Segnalazioni che, seppur non strettamente rilevanti ai sensi del D.lgs. 231/2001, siano comunque ritenute fondate.

Con periodicità annuale (se non diversamente richiesto), l'OdV fornisce all'Organo Amministrativo un apposito report riepilogativo delle Segnalazioni eventualmente pervenute contenente gli esiti delle analisi, inclusa l'adozione (o la mancata adozione) di provvedimenti disciplinari.

8.6 Conservazione della documentazione

Al fine di garantire la gestione e la tracciabilità delle Segnalazioni e delle relative attività, l'Organismo di Vigilanza cura l'attività di protocollo delle Segnalazioni, la predisposizione e l'aggiornamento di tutte le informazioni riguardanti le Segnalazioni ed assicura l'archiviazione di tutta la correlata documentazione di supporto per due anni dalla ricezione della Segnalazione.

8.7 Forme di tutela del whistleblower

A) Obblighi di riservatezza sull'identità del whistleblower e sottrazione al diritto di accesso della segnalazione

Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codice civile e delle ipotesi in cui l'anonimato non è opponibile per legge (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo) l'identità del *whisteblower* viene protetta in ogni contesto successivo alla Segnalazione.

Pertanto, fatte salve le eccezioni di cui sopra, l'identità del segnalante non può essere rivelata senza il suo espresso consenso e tutti coloro che ricevono o sono coinvolti nella gestione della Segnalazione sono tenuti a tutelare la riservatezza di tale informazione.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare e legittima l'applicazione da parte della Società delle sanzioni previste nella Sezione 4 del presente Modello, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

Per quanto concerne, in particolare, l'ambito del procedimento disciplinare, l'identità del segnalante può essere rivelata all'autorità disciplinare e all'incolpato solo nei casi in cui:

- vi sia il consenso espresso del segnalante;

- la contestazione dell'addebito disciplinare risulti fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato, sempre che tale circostanza venga da quest'ultimo dedotta e comprovata in sede di audizione o mediante la presentazione di memorie difensive.

B) Divieto di discriminazione nei confronti del whistleblower

Nei confronti del segnalante che effettua una Segnalazione ai sensi della presente Procedura non è consentita, né tollerata alcuna forma di ritorsione o misura

discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia.

Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili. Colui che ritiene di aver subito una discriminazione per il fatto di aver effettuato una segnalazione di illecito deve dare notizia circostanziata dell'avvenuta discriminazione al Responsabile Amministrativo che, valutata la sussistenza degli elementi, segnala l'ipotesi di discriminazione all'organo amministrativo per l'adozione dei provvedimenti del caso.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le Segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

8.8. Responsabilità del whistleblower

La presente Procedura di *Whistleblowing* lascia impregiudicata la responsabilità penale e disciplinare del *whistleblower* nell'ipotesi di Segnalazione calunniosa o diffamatoria ai sensi del codice penale e dell'art. 2043 del codice civile.

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente Procedura di *Whistleblowing*, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare

il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente Procedura di *Whistleblowing*.

****