

Modello Organizzativo e di Gestione (MOG) ai sensi del DLgs 231/2001 per Energie Salentine S.p.A.

PARTE I

ASPETTI GENERALI

1. Il DLgs 8 giugno 2001 n. 231 e l'imperativo per un MOG Solido

1.1. Il Decreto Legislativo 8 giugno 2001, n. 231.

Il dlgs. n. 231/2001 ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali, quali la *Convenzione di Bruxelles* del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la *Convenzione di Bruxelles* del 26 maggio 1997 sulla lotta alla corruzione e la *Convenzione OCSE* del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Con tale decreto, dedicato alla “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*”, si è ritenuto necessario introdurre nell’ordinamento italiano un regime di responsabilità amministrativa a carico degli enti per alcuni reati (c.d. “reati presupposto”) commessi, nell'interesse o vantaggio degli stessi enti:

- (i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi (cd. soggetti apicali),
- (ii) da persone fisiche o giuridiche sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (cd. soggetti sottoposti).

In particolare, l’individuazione dei cd. soggetti apicali deve essere effettuata tenendo conto della funzione in concreto svolta nell’ambito delle proprie mansioni e, dunque, della capacità di esercitare una influenza significativa sulla società o su una sua unità produttiva.

Per i cd. soggetti sottoposti, si ha riguardo a coloro che sono legati all’ente da rapporto di lavoro subordinato, parasubordinato nonché a collaboratori esterni, compresi fornitori o consulenti.

Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto e mira a coinvolgere gli enti nella punizione di taluni reati commessi nel loro interesse o a loro vantaggio.

Tra le sanzioni previste, oltre a quelle pecuniarie, le più gravi sono rappresentate da misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la P.A., l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

La responsabilità prevista dal suddetto Decreto si configura anche in relazione ai reati commessi all'estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato medesimo.

La responsabilità sorge già con riguardo ai reati arrestatisi allo stadio del tentativo. L'art. 26, comma 1, del dlgs 231/2001, stabilisce che, nei casi di realizzazione nella forma di tentativo dei delitti indicati, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre ne è esclusa l'irrogazione nei casi in cui l'ente *"impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento"*.

Quanto alla tipologia di reati destinati a comportare il suddetto regime di responsabilità amministrativa a carico degli Enti, il Decreto – nel testo originario – si riferiva ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione, ponendosi pertanto come obiettivo peculiare quello di sanzionare condotte di tipo corruttivo volte ad agevolare l'attività d'impresa.

Nel corso degli anni, l'elenco dei cd. reati-presupposto si è notevolmente esteso fino a ricomprendere gran parte delle fattispecie illecite riconducibili all'attività d'impresa.

Nel presente Modello verranno prese in considerazione solo le fattispecie di reato per le quali si rilevi un possibile livello di rischio rispetto alle attività svolte dalla società Energie Salentine S.p.A.

1.2. L'imperativo per un MOG Solido

Il Decreto Legislativo 8 giugno 2001, n. 231, ha introdotto un cambiamento significativo nella responsabilità aziendale, stabilendo un regime di responsabilità amministrativa per gli enti giuridici, comprese le società per azioni, per specifici tipi di reati commessi nel loro interesse o a loro vantaggio. Questa responsabilità è distinta e aggiuntiva rispetto alla responsabilità penale delle persone fisiche che commettono i reati.

Per una società per azioni, l'adozione di un efficace Modello Organizzativo e di Gestione (MOG) non è semplicemente una questione di conformità generale alle norme: è un imperativo strategico!

Invero, il decreto prevede che gli enti e quindi anche le società per azioni, per essere esenti da responsabilità, devono anzitutto dimostrare di aver adottato e attuato efficacemente un MOG idoneo a prevenire il tipo di reato commesso.

Oltre a questa cruciale difesa legale, un MOG funge da dimostrazione tangibile dell'impegno dell'azienda a prevenire attività criminali e promuovere una condotta etica all'interno delle sue operazioni. Stabilendo protocolli chiari, responsabilità e meccanismi di controllo, un MOG ben progettato può mitigare significativamente il rischio di incorrere in sanzioni potenzialmente gravi in caso di reato.

Inoltre, l'adozione e l'implementazione diligente di un MOG possono migliorare la reputazione dell'azienda tra gli *stakeholder*, favorendo una maggiore fiducia nella sua *governance* e nelle sue operazioni.

2. Principi fondamentali e quadro giuridico del DLgs 231/2001

Il dlgs 231/2001 prevede specifiche condizioni in base alle quali un ente può essere esonerato da responsabilità.

Per i reati commessi da persone in posizioni di vertice, l'ente deve provare di aver adottato e attuato efficacemente un MOG idoneo prima della commissione del reato.

Inoltre, il compito di vigilare sul funzionamento e l'osservanza del MOG, nonché di assicurare il suo aggiornamento periodico, deve essere stato affidato a un Organismo di Vigilanza (OdV) dotato di autonomi poteri di iniziativa e di controllo.

L'ente deve anche dimostrare che le persone hanno commesso il reato eludendo fraudolentemente il MOG e che non vi è stata omissione o insufficiente vigilanza da parte dell'OdV.

Per i reati commessi da persone sottoposte alla direzione o supervisione di persone in posizioni di vertice, l'ente può essere ritenuto responsabile solo se la commissione del reato è stata resa possibile da una mancanza di gestione o supervisione, a meno che un MOG idoneo non fosse in vigore prima del reato.

Un MOG idoneo è caratterizzato da diversi elementi chiave.

Esso deve identificare le specifiche attività all'interno dell'organizzazione in cui potrebbero potenzialmente essere commessi reati e specificare protocolli e procedure che guidano i processi decisionali e l'attuazione delle attività dell'ente in relazione alla prevenzione dei reati identificati, stabilendo, possibilmente, i metodi per la gestione delle risorse finanziarie dell'azienda in modo da prevenire efficacemente la commissione di reati.

Una componente cruciale del MOG è la creazione di flussi informativi obbligatori verso l'OdV, garantendo che l'organismo di vigilanza sia tenuto informato sulle attività rilevanti e sui potenziali rischi.

Il MOG efficace deve incorporare, tra i propri allegati, anche un Codice Etico, che delinea i principi e i valori fondamentali che dovrebbero guidare la condotta dell'azienda e del suo personale, nonché includere anche un sistema disciplinare in grado di sanzionare le persone che non rispettano le misure e le procedure delineate nel modello.

Infine, il MOG richiede una verifica periodica della sua implementazione e idoneità, nonché aggiornamenti per riflettere i cambiamenti nella legge o nelle operazioni dell'azienda

Il quadro giuridico sottolinea che la mera esistenza di un Modello Organizzativo e di Gestione sulla carta non è sufficiente per assolvere l'ente da responsabilità. Il suo vero valore risiede nella sua efficace attuazione e nella supervisione continua fornita da un Organismo di Vigilanza indipendente.

Il ruolo attivo dell'OdV nel monitorare la conformità e prevenire l'elusione fraudolenta è un fattore critico per dimostrare l'efficacia del MOG e l'impegno dell'ente alla due diligence.

Inoltre, l'attenzione del decreto sui reati commessi nell'"interesse o vantaggio" dell'ente richiede che il MOG consideri non solo i benefici diretti per l'azienda, ma anche scenari in cui le persone potrebbero agire in nome dell'azienda anche con motivazioni miste.

Il processo di valutazione del rischio deve quindi esplorare potenziali conflitti di interesse e situazioni in cui il confine tra guadagno individuale e aziendale potrebbe essere sfumato, garantendo che il MOG affronti adeguatamente queste complessità.

3. Valutazione completa del rischio per la Società per Azioni.

Per sviluppare un MOG efficace, Energie Salentine S.p.A. deve condurre una valutazione approfondita del rischio per identificare le aree all'interno delle sue operazioni potenzialmente vulnerabili alla commissione di reati presupposto ai sensi del dlgs 231/2001.

Questi ultimo includono reati contro la Pubblica Amministrazione, reati societari, reati ambientali, abuso di mercato, terrorismo e sovversione, reati contro la persona, omicidio colposo e lesioni dovute a violazioni della sicurezza, ricettazione, riciclaggio di denaro, autoriciclaggio, violazione del diritto d'autore, induzione a non rendere dichiarazioni, reati informatici e trattamento dati, reati relativi agli strumenti di pagamento, impiego di immigrati clandestini, frode sportiva, reati tributari, contrabbando, reati contro il patrimonio culturale e manipolazione del mercato.

Considerando la struttura organizzativa di Energie Salentine S.p.A., comprendente un consiglio di amministrazione, un direttore generale, e quattro aree funzionali, rispettivamente area comunicazione istituzionale, area tecnica, area relazioni pubbliche e ai rapporti internazionali ed area amministrativa, la valutazione del rischio dovrebbe concentrarsi specificamente sulle seguenti aree funzionali:

- **Comunicazione Istituzionale:** quest'area comporta potenziali rischi legati all'immagine pubblica e alla posizione di mercato dell'azienda. Reati come la manipolazione del mercato e le false comunicazioni sociali potrebbero derivare da dichiarazioni pubbliche fuorvianti o inaccurate. Si configura, altresì, il rischio di comportamenti corruttivi o inducibili o, in generale, di realizzazione di delitti contro la Pubblica Amministrazione, che impone una particolare attenzione al fine di prevenire, attenuare e, auspicabilmente, eliminare quel rischio.
- **Area Tecnica:** le operazioni tecniche dell'azienda possono essere esposte a rischi relativi a comportamenti che possano dar luogo a delitti contro la Pubblica Amministrazione, nella misura in cui l'Area Tecnica venga coinvolta in procedure di gara o di negoziazione indette da enti pubblici nazionali o esteri per l'assegnazione di commesse, di concessioni, o per la erogazione di contributi o finanziamenti. L'Area Tecnica è altresì esposta al rischio di reati frode in pubbliche forniture, di truffa aggravata, e rischio di concorrere nella realizzazione di reati tributari e societari, nel riciclaggio, auto riciclaggio di danaro e fattispecie similari. Trattasi, invero, di un'Area che svolge attività trasversale, venendo interessata a tutte le fasi dell'azione della società Energie Salentine, ivi compresa l'attività di vigilanza e controllo sulla realizzazione delle opere, sulla rendicontazione dei contributi, sui pareri tecnici di varia natura.
- **Relazioni Pubbliche e Internazionali:** questa funzione è particolarmente suscettibile a rischi di corruzione e concussione nei rapporti con i funzionari pubblici a livello nazionale e internazionale, nonché con i *partner* esterni. Esiste anche un potenziale per reati relativi all'indebita induzione in queste interazioni.
- **Amministrazione:** le funzioni amministrative dell'azienda sono esposte a rischi di corruzione e concussione, ed a vulnerabilità nella gestione finanziaria, che potrebbe portare

a frodi ai danni dello Stato o di altri enti pubblici, nonché all'evasione fiscale. Inoltre, esiste il rischio di reati societari relativi alle pratiche contabili, come la falsa contabilità e la comunicazione finanziaria fraudolenta. Qualche raro rischio potrebbe anche individuarsi nell'attività di gestione del personale.

Il processo di valutazione del rischio deve essere dinamico e continuo, riconoscendo che il panorama giuridico e le operazioni dell'azienda si evolveranno nel tempo. L'elenco dei reati presupposto ai sensi del DLgs 231/2001 è stato soggetto a modifiche e aggiunte dalla sua entrata in vigore, rendendo necessari aggiornamenti periodici del MOG. Inoltre, i cambiamenti nelle attività commerciali dell'azienda, nella struttura organizzativa o nell'ambiente normativo possono introdurre nuovi rischi o alterare la probabilità e l'impatto di quelli esistenti. La valutazione del rischio dovrebbe considerare sia i criteri di "interesse" che di "vantaggio" delineati nel decreto. L'"interesse" comporta una valutazione prospettica del beneficio previsto per l'ente al momento del reato, mentre il "vantaggio" si riferisce a qualsiasi beneficio o guadagno che l'ente ha effettivamente tratto dalla commissione del reato. Questa duplice prospettiva è cruciale per un'identificazione completa di tutti i potenziali rischi.

Per fornire una chiara panoramica della valutazione del rischio, la seguente tabella riassume le aree di rischio identificate e la mappa dei potenziali reati presupposto ai sensi del dlgs 231/2001:

Area Funzionale	Attività Specifiche all'Interno dell'Area	Potenziali Reati Presupposto (con Articolo del DLgs 231/2001)
Comunicazione Istituzionale	Dichiarazioni pubbliche, comunicati stampa, relazioni con gli investitori, documenti normativi	False comunicazioni sociali (Art. 25-ter), Induzione a non rendere dichiarazioni (Art. 25-decies), Peculato, indebita destinazione di denaro, corruzione, traffico di influenze (Art. 25)
Area Tecnica	Progettazione e sviluppo prodotti e servizi, controllo e vigilanza sulla realizzazione del progetto e sulla rendicontazione, vigilanza sui collaboratori esterni	Peculato, indebita destinazione di denaro, corruzione, traffico di influenze (Art. 25), Riciclaggio di Denaro (Art. 25-octies) Frode ai Danni dello Stato o di Enti Pubblici (Art. 24),
Relazioni Pubbliche e Internazionali	Interazioni con funzionari pubblici, attività di <i>lobbying</i> , <i>partnership</i> internazionali, sponsorizzazioni, donazioni	Corruzione e Concussione (Art. 25), Indebita Induzione (Art. 25), Traffico di Influenze (Art. 25)
Amministrazione	Reporting finanziario, contabilità, conformità fiscale, approvvigionamento, gestione del personale, gestione contratti, vigilanza e gestione fondi pubblici	Frode ai danni dello Stato o di Enti Pubblici (Art. 24), Reati Tributari (Art. 25-quinquiesdecies), Reati Societari (Art. 25-ter), Peculato, indebita destinazione di denaro, corruzione, traffico di influenze (Art. 25), Riciclaggio di denaro (Art. 25-octies)

4. Struttura organizzativa, responsabilità e delega di autorità per la prevenzione dei reati

Un aspetto fondamentale per stabilire un MOG efficace è una chiara comprensione della struttura organizzativa, delle responsabilità di ciascun ruolo e dell'appropriata delega di autorità, in particolare in relazione alla prevenzione della commissione di reati ai sensi del dlgs 231/2001.

Il **Consiglio di Amministrazione** detiene la responsabilità ultima per l'adozione e la supervisione dell'implementazione e dell'efficacia del MOG. Questa responsabilità non è delegabile per quanto riguarda l'adozione e l'aggiornamento del modello. Il Consiglio è anche responsabile della nomina

dei membri dell'Organismo di Vigilanza. Il loro ruolo si estende oltre l'adozione iniziale del MOG, per garantirne l'efficacia continua attraverso la fornitura delle risorse e del supporto necessari all'OdV.

Il **Direttore Generale** svolge un ruolo cruciale nell'implementazione e nell'applicazione del MOG in tutte le aree operative dell'azienda. Ciò include l'esigenza di garantire che tutto il personale sia a conoscenza e rispetti i principi e le procedure delineate nel MOG, nonché di promuovere una cultura di condotta etica e conformità all'interno della propria sfera di competenza.

I **Responsabili dell'Area Tecnica e dell'Area della Comunicazione Istituzionale** sono chiamati a garantire la conformità al MOG all'interno delle rispettive aree funzionali. Ciò comporta l'implementazione di protocolli e controlli specifici pertinenti ai rischi identificati all'interno della propria Area Funzionale e garantire che i loro *team* siano adeguatamente formati e consapevoli delle loro responsabilità ai sensi del MOG.

Il **Responsabile dell'Area delle Relazioni Pubbliche e Rapporti Internazionali** deve aderire ai più elevati *standard* di condotta etica in tutte le interazioni esterne. Questo ruolo richiede una conoscenza approfondita del MOG dell'azienda e dei requisiti legali pertinenti per gestire i rapporti con i funzionari pubblici e i *partner* internazionali in modo pienamente conforme, evitando qualsiasi azione che possa essere interpretata come corruzione, concussione o indebita induzione.

Il **Responsabile dell'Area Amministrativa** deve curare e garantire il mantenimento di processi amministrativi trasparenti e conformi alle regole giuridiche ed alle disposizioni interne. Ciò include la tenuta di una corretta documentazione e delle autorizzazioni eventualmente necessarie per porre in essere tutte le transazioni finanziarie, mantenere registri contabili accurati e rispettare le procedure di controllo interno stabilite per prevenire irregolarità finanziarie e potenziali reati, nonché il rispetto delle norme sulla gestione del personale.

Per garantire un'efficace prevenzione dei reati, l'azienda deve formalizzare ruoli, responsabilità e linee di *reporting* attraverso organigrammi e descrizioni di lavoro chiari. È anche essenziale un sistema ben definito di deleghe di autorità con limiti e responsabilità chiaramente definiti.

Inoltre, l'implementazione della segregazione dei compiti nei processi critici può ridurre significativamente il rischio di conflitti di interesse e opportunità di attività fraudolente. Una struttura organizzativa chiaramente definita con ruoli e responsabilità ben articolati fornisce il quadro necessario per l'efficace implementazione del MOG e l'allocazione della responsabilità per le misure preventive all'interno di ciascuna area funzionale. L'impegno attivo del Consiglio di Amministrazione nel garantire l'efficacia del MOG, compresa la fornitura di risorse e supporto adeguati all'OdV, è cruciale per promuovere una vera cultura della conformità in tutta l'organizzazione.

5. Il ruolo cruciale e le dinamiche operative dell'Organismo di Vigilanza (OdV)

Un elemento fondamentale di un MOG efficace ai sensi del dlgs 231/2001 è la costituzione di un Organismo di Vigilanza (OdV). L'articolo 6, comma 1, lett. b), del citato decreto impone la nomina

di un OdV con la responsabilità primaria di vigilare sul funzionamento e l'osservanza del MOG e di assicurare che sia tenuto aggiornato.

Per adempiere efficacemente al proprio mandato, l'OdV deve possedere alcune caratteristiche essenziali.

L'**autonomia e l'indipendenza** sono fondamentali, richiedendo che l'OdV operi indipendentemente dalla direzione aziendale e non sia soggetto a gerarchie interne o pressioni esterne. Questa indipendenza è sostenuta dal potere dell'OdV di accedere a tutte le informazioni e i documenti aziendali rilevanti necessari per le sue attività di supervisione.

Anche la **professionalità e la competenza** sono cruciali, richiedendo che i membri dell'OdV possiedano comprovata esperienza in aree quali il diritto penale, l'organizzazione aziendale e i modelli di prevenzione ai sensi del DLgs 231/2001. Essi devono rimanere costantemente aggiornati sulle normative pertinenti e sulle migliori pratiche in materia di conformità.

Inoltre, l'OdV deve garantire un'**azione continua**, essendo dotato di risorse adeguate e dedicando tempo sufficiente allo svolgimento diligente dei propri compiti.

L'OdV è nominato dall'organo amministrativo, che decide il numero e la qualifica dei componenti, sia interni sia esterni, sulla base delle dimensioni dell'ente, dell'attività svolta e delle aree nel cui ambito possono essere commessi i reati-presupposto, così come individuate dal modello organizzativo.

La nomina dei membri dell'OdV deve essere resa nota a ciascun componente nominato e da questi formalmente accettata con apposita dichiarazione che attesti, altresì, il possesso dei requisiti richiesti dalla norma.

La nomina dell'OdV per la prima volta avviene con la stessa delibera di approvazione e adozione del modello organizzativo. Successivamente, l'Organismo è rinnovato con apposita decisione dell'organo amministrativo e resta in carica per il numero di esercizi sociali da quest'ultimo stabilito all'atto di nomina.

L'Organismo nomina tra i suoi membri il Presidente, a cui sarà affidato il compito, tra gli altri, di espletare le formalità relative alla convocazione, alla fissazione degli argomenti da trattare, all'organizzazione e allo svolgimento delle riunioni collegiali.

Nelle società di capitali la funzione di OdV può essere attribuita, con apposita decisione dell'organo amministrativo, al collegio sindacale (art. 6, comma 4-bis, d.lgs. 231/2001). Le modalità di svolgimento della funzione di OdV da parte del collegio sindacale muovono dal presupposto che l'attribuzione della funzione di OdV avviene a favore dell'organo di controllo interno e non dei suoi singoli componenti, e che le duplici funzioni di vigilanza ex artt. 2403 ss. c.c. e di OdV ex dlgs. 231/2001, rimangono distinte, ma vanno coordinate fra di loro, realizzando opportune sinergie e garantendo maggiore efficienza operativa. Ne consegue che la natura di organo sociale del collegio sindacale è prevalente rispetto a quella funzionale di OdV. La disciplina e la metodologia dettate per quest'ultimo devono, pertanto, integrarsi con quelle proprie del collegio sindacale, il cui funzionamento è già regolamentato dalla legge e dallo statuto. Dunque, nei confronti del collegio

sindacale incaricato della funzione di OdV troveranno applicazione anche le norme del d.lgs. 231/2001.

L'OdV svolge una serie di compiti chiave per garantire l'efficacia del MOG. Questi includono il monitoraggio attivo della conformità al MOG e a tutte le procedure correlate e la conduzione di *audit* e verifiche periodiche per valutare la sua implementazione e il suo rispetto. L'OdV è anche responsabile della ricezione e dell'analisi approfondita di informazioni e segnalazioni relative a potenziali violazioni del MOG o di altre normative pertinenti e della segnalazione delle proprie attività e dei propri risultati direttamente al Consiglio di Amministrazione. In modo proattivo, l'OdV svolge un ruolo vitale nella promozione della consapevolezza e nella fornitura di formazione sul MOG in tutta l'organizzazione e nella gestione del processo di *whistleblowing* dell'azienda, garantendo un canale sicuro e confidenziale per la segnalazione di potenziali illeciti.

L'OdV deve mantenere una linea di *reporting* diretta ai massimi livelli di gestione (in genere al Consiglio di Amministrazione) per salvaguardare la sua indipendenza e garantire che le sue raccomandazioni siano debitamente prese in considerazione.

Il ruolo dell'OdV non è semplicemente quello di reagire a potenziali problemi, ma di promuovere attivamente una cultura della conformità e di cercare continuamente opportunità per migliorare l'efficacia del MOG, inclusa la partecipazione agli aggiornamenti della valutazione del rischio e allo sviluppo di nuovi protocolli preventivi.

6. Protocolli aziendali per la gestione dei processi sensibili e la mitigazione dei rischi di commissione di reati presupposto ai sensi del dlgs 231/2001

Lo sviluppo di solidi protocolli aziendali è essenziale per gestire efficacemente i processi sensibili e mitigare i rischi di commissione di reati presupposto ai sensi del dlgs 231/2001. Questi protocolli vanno adattati alle specifiche aree di rischio identificate nella valutazione del rischio e devono delineare chiaramente le procedure e i controlli da seguire.

Nella articolazione generale della Parte Speciale e nella analisi delle vicende connesse a determinate fattispecie di reato ritenute maggiormente a rischio per le peculiarità delle attività della società, si rinvengono indicazioni più specifiche, oltre a quanto qui di seguito osservato a livello generale.

I protocolli per l'**autorizzazione di spese e impegni** dovrebbero definire flussi di lavoro di approvazione e limiti di spesa chiari in base ai ruoli e alle responsabilità del personale. L'implementazione della segregazione dei compiti nel processo di approvvigionamento, in cui individui diversi sono responsabili dell'avvio, dell'approvazione, dell'esecuzione e della registrazione delle transazioni, può ridurre significativamente il rischio di attività non autorizzate o fraudolente.

I **controlli interni sulle transazioni finanziarie** dovrebbero stabilire controlli ed equilibri completi per tutti i pagamenti, le ricevute e i registri contabili. Ciò include garantire la tracciabilità di tutti i flussi finanziari, dall'inizio alla registrazione, per facilitare audit e indagini.

La **gestione dei rapporti con i funzionari pubblici e i partner esterni** richiede la definizione di chiare linee guida per tutte le interazioni, vietando esplicitamente la corruzione, la concussione e qualsiasi forma di indebita induzione. È inoltre fondamentale implementare procedure di *due diligence* approfondite per la selezione e la gestione dei *partner* esterni.

I protocolli per la **gestione delle informazioni riservate e la prevenzione delle violazioni dei dati** dovrebbero includere l'implementazione di solide misure di sicurezza IT, controlli di accesso rigorosi ai dati sensibili e politiche complete di protezione dei dati. Devono inoltre essere stabilite procedure chiare per la segnalazione e la gestione di eventuali violazioni dei dati che potrebbero verificarsi.

Infine, i protocolli per la **tenuta di registri accurati e trasparenti** sono essenziali per garantire che tutte le attività rilevanti siano adeguatamente documentate, l'integrità dei dati sia mantenuta e l'azienda sia in grado di facilitare efficacemente gli audit interni ed esterni.

7. Programmi strategici di formazione e sensibilizzazione sul MOG e sul dlgs 231/2001

La progettazione e l'implementazione di programmi di formazione e sensibilizzazione completi sono cruciali per garantire che il MOG sia efficacemente integrato nella cultura aziendale e che tutto il personale comprenda i propri ruoli e responsabilità nella prevenzione dei reati ai sensi del dlgs 231/2001.

Questi programmi di formazione dovrebbero coprire argomenti chiave come i principi fondamentali del dlgs 231/2001 e le sue implicazioni per l'azienda, una panoramica dettagliata del MOG specifico dell'azienda, inclusa la sua struttura, i principi e le procedure, una spiegazione approfondita dei reati presupposto rilevanti che l'azienda rischia di commettere in base alle sue operazioni, l'importanza di aderire a una condotta etica in tutte le attività aziendali e i meccanismi di segnalazione stabiliti, inclusa la politica di *whistleblowing*, per sollevare preoccupazioni su potenziali violazioni.

È essenziale condurre queste sessioni di formazione regolarmente e documentare meticolosamente la loro occorrenza e il loro contenuto. La formazione dovrebbe essere specificamente adattata e calibrata in base al livello di responsabilità e ai compiti specifici del personale che riceve la formazione. Ad esempio, i dipendenti in aree ad alto rischio o quelli con significativa autorità decisionale potrebbero richiedere una formazione più approfondita e specializzata rispetto agli individui in ruoli meno sensibili. Per garantire l'efficacia della formazione, dovrebbero essere implementati controlli periodici, comprese valutazioni intermedie, per valutare il livello di comprensione raggiunto dai partecipanti.

L'azienda dovrebbe considerare l'adozione di un approccio misto alla fornitura di formazione, sfruttando i vantaggi sia delle sessioni in aula di persona, che consentono l'interazione diretta e la discussione, sia delle moderne piattaforme di *e-learning*, che offrono flessibilità e accessibilità, consentendo al personale di accedere ai materiali di formazione al proprio ritmo e convenienza. Questo approccio strategico alla formazione e alla sensibilizzazione è fondamentale per promuovere una vera cultura della conformità e del comportamento etico in tutta l'organizzazione.

8. Stabilire procedure efficaci per l'aggiornamento periodico e la verifica dell'efficacia del MOG

Per garantirne la continua rilevanza ed efficacia, il MOG deve essere trattato come un "*documento vivente*" soggetto ad aggiornamenti e verifiche periodiche. Diversi fattori dovrebbero indurre una revisione e un potenziale aggiornamento del MOG. Questi includono modifiche legislative che introducono nuovi reati presupposto o modificano quelli esistenti, significative ristrutturazioni organizzative all'interno dell'azienda, l'identificazione di rischi nuovi o emergenti attraverso il monitoraggio continuo o le valutazioni del rischio e casi di non conformità al MOG o alle normative pertinenti.

L'azienda dovrebbe stabilire procedure chiare per la verifica periodica dell'efficacia del MOG. Ciò può essere ottenuto attraverso vari metodi, tra cui *audit* interni regolari condotti dall'OdV o da una funzione di *audit* interno e la rivalutazione periodica dei rischi per identificare nuove vulnerabilità o cambiamenti nel panorama dei rischi.

L'Organismo di Vigilanza svolge un ruolo centrale nella supervisione sia dei processi di aggiornamento che di verifica del MOG. Sebbene alcune linee guida suggeriscano revisioni annuali del MOG, la frequenza effettiva degli aggiornamenti dovrebbe essere principalmente guidata dal verificarsi di cambiamenti significativi all'interno dell'azienda o nell'ambiente legale. La posizione indipendente dell'OdV gli consente di valutare obiettivamente la necessità di aggiornamenti e di monitorarne l'efficace implementazione, garantendo che il MOG rimanga uno strumento rilevante e robusto per la prevenzione dei reati e la mitigazione del rischio di responsabilità dell'azienda.

9. Comprendere lo spettro delle sanzioni per la mancata adozione o l'implementazione inefficace del MOG

La mancata adozione di un MOG efficace o l'averne uno che non sia implementato efficacemente può esporre la società per azioni a sanzioni significative ai sensi del DLgs 231/2001 se un reato presupposto viene commesso nel suo interesse o a suo vantaggio. Queste sanzioni possono essere sia di natura finanziaria che operativa.

Le **sanzioni pecuniarie** sono sempre applicate quando un ente è ritenuto responsabile ai sensi del dlgs 231/2001. Queste sanzioni sono calcolate utilizzando un sistema di quote, con il numero di quote che va da un minimo di 100 a un massimo di 1000. Il valore assegnato a ciascuna quota può variare da € 258,23 a € 1549,37, a seconda delle condizioni economiche e finanziarie dell'ente. Ciò si traduce in potenziali multe che vanno da € 25.823,00 a € 1.549.370,00.

Oltre alle sanzioni pecuniarie, il decreto prevede una serie di **sanzioni interdittive**, che possono incidere gravemente sulle operazioni dell'azienda. Queste includono l'interdizione temporanea o definitiva dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni necessarie per le operazioni dell'azienda, il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi pubblici, con la potenziale revoca di eventuali benefici precedentemente concessi, e il divieto di pubblicizzare beni o servizi. In casi particolarmente gravi, le sanzioni interdittive possono essere applicate in modo definitivo, come il

divieto permanente di esercitare attività imprenditoriali, soprattutto se l'azienda ha tratto un profitto significativo dal reato e ha una storia di ripetuti divieti temporanei.

Inoltre, il decreto impone la **confisca dei profitti o dei proventi del reato** in caso di condanna. Il tribunale può anche ordinare la **pubblicazione della sentenza di condanna**, che può comportare un significativo danno reputazionale per l'azienda.

La gravità delle sanzioni applicate dipenderà da fattori quali la gravità del reato, il livello di responsabilità delle persone coinvolte e la misura in cui l'azienda ha adottato misure per prevenire la commissione di tali reati.

In particolare, l'adozione e l'efficace implementazione di un MOG *prima* della commissione di un reato possono, a determinate condizioni, esentare l'azienda da responsabilità, soprattutto se il reato è stato commesso eludendo fraudolentemente il MOG e non vi è stata mancanza di vigilanza da parte dell'OdV. Ciò sottolinea la fondamentale importanza della conformità proattiva per evitare queste conseguenze finanziarie e operative potenzialmente devastanti. Anche dopo che si è verificato un reato, dimostrare un impegno alla conformità attraverso un MOG efficace può potenzialmente influenzare la gravità delle sanzioni imposte dalle autorità giudiziarie.

10. Conclusione: Implementare un MOG Sostenibile ed Efficace per la Conformità a Lungo Termine

La creazione di un Modello Organizzativo e di Gestione conforme al DLgs 231/2001 per una società per azioni è un processo multiforme che richiede una profonda comprensione dei requisiti legali, una valutazione approfondita dei rischi specifici dell'azienda, una struttura organizzativa ben definita con chiare responsabilità, la costituzione di un Organismo di Vigilanza robusto e indipendente, lo sviluppo di protocolli aziendali su misura per i processi sensibili, programmi strategici di formazione e sensibilizzazione per tutto il personale e procedure efficaci per l'aggiornamento periodico e la verifica dell'efficacia del MOG.

Il percorso verso la conformità non è un progetto *una tantum*, ma un impegno continuo. Affinché il MOG rimanga efficace e fornisca una solida difesa contro la potenziale responsabilità, la società per azioni deve abbracciare una cultura del miglioramento continuo, rivedendo e aggiornando regolarmente il MOG per riflettere i cambiamenti nella legislazione, nelle operazioni aziendali e nel panorama dei rischi in evoluzione. Il coinvolgimento attivo e l'indipendenza dell'Organismo di Vigilanza sono fondamentali per garantire l'integrità e l'efficacia del MOG nel tempo.

I prossimi passi in questo processo di implementazione dovrebbero includere:

1. **Condurre una valutazione del rischio completa e dettagliata** su misura per la sua specifica struttura organizzativa e attività operative, concentrandosi sulle aree funzionali della comunicazione istituzionale, delle attività tecniche, delle relazioni pubbliche e internazionali e dell'amministrazione.
2. **Sviluppare e formalizzare ruoli, responsabilità e linee di autorità chiari** per tutto il personale in relazione alla prevenzione dei reati presupposto.
3. **Costituire un Organismo di Vigilanza indipendente e professionalmente competente** dotato di autonomi poteri di iniziativa e di controllo.

4. **Progettare e implementare protocolli aziendali specifici** per la gestione dei processi sensibili all'interno delle aree di rischio identificate, concentrandosi su autorizzazione, controllo, tracciabilità e interazioni con parti esterne.
5. **Creare ed erogare programmi strategici di formazione e sensibilizzazione** sul dlgs 231/2001 e sul MOG dell'azienda per tutti i livelli di personale, garantendo che la formazione sia specifica per il ruolo e regolarmente aggiornata.
6. **Stabilire procedure chiare per l'aggiornamento periodico e la verifica dell'efficacia del MOG**, con l'OdV che svolge un ruolo centrale di supervisione in questo processo.

Intraprendendo diligentemente questi passaggi e promuovendo una forte cultura dell'etica e della conformità, la Energie Salentine S.p.A. può realizzare un Modello Organizzativo e di Gestione sostenibile ed efficace che non solo soddisfi i requisiti del dlgs 231/2001, ma fornisca anche una solida difesa contro la responsabilità amministrativa, salvaguardando il successo e la reputazione a lungo termine dell'azienda.

Modello Organizzativo e di Gestione (MOG) ai sensi del DLgs 231/2001 per Energie Salentine S.p.A.

PARTE II

IL MODELLO DI ENERGIE SALENTINE S.P.A.

Articolazione generale

INDICE

1. **Premessa**
 - 1.1 Finalità del Modello
 - 1.2 Destinatari del Modello
 - 1.3 Aggiornamento del Modello
 - 1.4 Documenti di Riferimento
2. **Società, Attività Sensibili e Rischi**
 - 2.1 Struttura Societaria e Governance
 - 2.2 Attività a Rischio di Reato
 - 2.3 Mappatura dei Rischi Specifici
3. **Principi Generali di Comportamento**
 - 3.1 Codice Etico
 - 3.2 Principi di Trasparenza e Correttezza
 - 3.3 Principi di Diligenza e Prudenza
 - 3.4 Conflitti di Interesse
4. **Sistema di Controllo Interno**
 - 4.1 Organismo di Vigilanza (OdV)
 - 4.1.1 Composizione, Nomina e Durata in Carica
 - 4.1.2 Poteri e Responsabilità
 - 4.1.3 Flussi Informativi verso l'OdV
 - 4.2 Funzioni di Controllo
 - 4.2.1 Internal Audit
 - 4.2.2 Compliance
 - 4.2.3 Risk Management
 - 4.3 Sistema di Deleghe e Procure
5. **Aree Funzionali Sensibili e Protocolli**
 - 5.1 Area Tecnica
 - 5.1.1 Protocolli Specifici
 - 5.2 Area Comunicazione Istituzionale e Politica
 - 5.2.1 Protocolli Specifici
 - 5.3 Area Relazioni Pubbliche e Internazionali
 - 5.3.1 Protocolli Specifici
 - 5.4 Area Amministrazione
 - 5.4.1 Protocolli Specifici
6. **Attività Sensibili e Protocolli**
 - 6.1 Gestione del personale
 - 6.1.1 I rischi reato
 - 6.1.2 Procedure e protocolli
 - 6.2 Selezione e contrattualizzazione del personale e/o di professionisti
 - 6.2.1 I rischi reato
 - 6.2.2 Procedure e protocolli

- 6.3 Gestione delle procedure di gara o di negoziazione indette da enti pubblici nazionali o esteri per l'assegnazione di commesse, di concessioni o per la erogazione di contributi o finanziamenti. Gestione dei relativi contratti e convenzioni. Gestione del processo di approvvigionamento di beni e servizi
 - 6.3.1 I rischi reato
 - 6.3.2 Procedure e protocolli
 - 6.3.2.1 Ambito
 - 6.3.2.2 Selezione e qualifica dei fornitori
 - 6.3.2.3 Contratti e clausole risolutive
 - 6.3.2.4 *Due diligence*
 - 6.4 Gestione delle attività di pubbliche relazioni
 - 6.4.1 I rischi reato
 - 6.4.2 Procedure e protocolli
 - 6.5 Gestione dei sistemi informatici
 - 6.5.1 I rischi reato
 - 6.5.2 Procedure e protocolli
 - 6.6 Gestione finanziaria e contabile. Attività di formazione e approvazione del bilancio
 - 6.6.1 I rischi reato
 - 6.6.2 Procedure e protocolli
 - 6.7 Gestione dei fondi pubblici e rendicontazione
 - 6.7.1 I rischi reato
 - 6.7.2 Procedure e protocolli
 - 6.7.2.1 Procedure per l'utilizzo dei Fondi
 - 6.7.2.2 Controlli sulla rendicontazione
 - 6.7.2.3 Tracciabilità dei pagamenti
 - 6.7.2.4 Rapporti con gli enti erogatori
 - 6.1 Gestione del personale
 - 6.1.1 I rischi reato
 - 6.1.2 Procedure e protocolli
7. **Sistema disciplinare**
- 7.1 Sanzioni per violazioni del Modello
 - 7.2 *Whistleblowing*
8. **Formazione e Informazione**
- 8.1 Programmi di formazione
 - 8.2 Diffusione del Modello
9. **Monitoraggio e aggiornamento del Modello**
- 9.1 Attività di monitoraggio dell'OdV
 - 9.2 Revisione e aggiornamento del Modello
10. **Allegati**
- Codice Etico
 - Organigramma Societario
 - Matrice dei Rischi

* * * * *

1. Premessa

1.1 Finalità del Modello

Il presente Modello di Organizzazione, Gestione e Controllo (di seguito, "Modello") è adottato dalla società Energie Salentine S.p.A. (di seguito, "Società"), in conformità al dlgs. 8 giugno 2001, n. 231 (di seguito, "Decreto 231"), al fine di prevenire la commissione dei reati previsti dal decreto stesso e di promuovere una cultura aziendale improntata all'etica, alla legalità e alla trasparenza.

Il Modello mira a proteggere la Società da responsabilità amministrative derivanti da reati commessi nel suo interesse o a suo vantaggio da soggetti apicali (amministratori, dirigenti) o da soggetti sottoposti alla direzione o vigilanza di questi ultimi (dipendenti, collaboratori).

Gli obiettivi specifici del Modello sono:

- Prevenire la commissione dei reati previsti dal dlgs 231/2001

- Promuovere una cultura aziendale di integrità, etica e rispetto delle leggi.
- Proteggere la reputazione e il valore della Società.
- Assicurare la conformità normativa.
- Favorire la trasparenza e la responsabilità nelle operazioni aziendali.

L'art. 6, comma 2, lett. a), del D.Lgs. n. 231/2001 prevede che il Modello debba individuare le attività nel cui ambito possono essere commessi i reati presupposto. In coerenza con tale previsione, Energie Salentine S.p.A. ha provveduto a identificare le attività c.d. "a rischio" e le singole aree della Società nel cui ambito potrebbero essere commessi i reati attraverso l'attività di mappatura richiamata nella Parte Generale del presente Modello.

L'esame preliminare delle attività e del contesto in cui opera la Società, ha consentito innanzitutto di identificare le fattispecie di reato ragionevolmente configurabili nell'ambito della realtà aziendale.

È stata, infatti, effettuata un'analisi preliminare, considerando tutte le fattispecie di reato richiamate dal D.Lgs. 231/2001 (di seguito il "Decreto"), per valutare se in linea teorica le fattispecie richiamate possano anche solo astrattamente essere configurabili rispetto alle specificità delle attività svolte dalla Società, alle caratteristiche del sistema organizzativo adottato ed alla configurazione giuridica della Società medesima.

A seguito di detta analisi preliminare, sono state ragionevolmente escluse a priori determinate fattispecie di reato in quanto ritenute non astrattamente applicabili alla realtà di Energie Salentine S.p.A. In ragione di ciò, rispetto alle fattispecie escluse, non è stata effettuata la successiva analisi di dettaglio volta a determinare l'area aziendale nel cui ambito i rischi-reato possano configurarsi ed i relativi livelli di controllo, limitati, pertanto, alle sole fattispecie rilevanti per la Società.

1.2 Destinatari del Modello:

Il Modello si applica a tutti i membri del Consiglio di Amministrazione, al Direttore Generale, ai dirigenti, ai dipendenti, ai collaboratori, ai consulenti, agli agenti, ai procuratori, ai fornitori, e a tutti coloro che agiscono in nome e per conto della Società, sia in Italia che all'estero.

Tutti i Destinatari sono tenuti a conoscere, comprendere e rispettare il Modello. La violazione del Modello può comportare sanzioni disciplinari.

1.3 Aggiornamento del Modello:

Il Modello è soggetto a revisione periodica, almeno annualmente, e ad aggiornamenti in caso di modifiche normative, cambiamenti nella struttura aziendale, nuove aree di rischio, segnalazioni di violazioni, o risultati di *audit* interni o esterni.

L'Organismo di Vigilanza (OdV) è responsabile della revisione e dell'aggiornamento del Modello, in collaborazione con il CdA e le aree funzionali competenti.

1.4 Documenti di Riferimento:

Il Modello deve essere letto e interpretato congiuntamente ai seguenti documenti:

- Codice Etico (Allegato 1)
- Organigramma Societario (Allegato 2)
- Matrice dei Rischi (Allegato 3)

2. Società, attività sensibili e rischi

2.1 Struttura societaria e *governance*

La Società Energie Salentine è una Società per Azioni (S.p.A.) con sede legale in Verona via Antonio Locatelli 1 cap 37122.

La società è amministrata da un Consiglio di Amministrazione (CdA), composto da cinque membri, tra cui il Presidente, con poteri di indirizzo strategico, gestione ordinaria e straordinaria e controllo.

Ha un Direttore Generale (DG), responsabile dell'attuazione delle strategie e della gestione operativa.

L'Organismo di Vigilanza (OdV), quale organo di controllo interno con funzioni di vigilanza sull'applicazione del Modello 231/2001, viene nominato dal Consiglio di Amministrazione unitamente all'approvazione del predetto Modello.

La società si articola nelle seguenti Aree funzionali:

- Area Tecnica
- Area Comunicazione Istituzionale e Politica
- Area Relazioni Pubbliche e Internazionali
- Area Amministrazione

Ha un Organigramma Societario molto snello, come illustrato nella scheda allegata alla presente, che ne illustra la struttura organizzativa e le relazioni gerarchiche (all. 2).

2.2 Attività a rischio di reato

Le attività aziendali che possono essere considerate a rischio di reato includono, a titolo esemplificativo:

- Acquisizione di autorizzazioni e concessioni pubbliche per la costruzione e gestione dell'impianto di idrogeno verde nonché per l'acquisizione di aree annesse e connesse.
- Gestione di appalti e contratti con fornitori di beni e servizi per la costruzione e manutenzione dell'impianto.
- Attività di *lobbying* e relazioni istituzionali con enti pubblici e politici.
- Gestione di fondi pubblici e rendicontazione delle spese.
- Gestione di dati sensibili e informazioni riservate relative a progetti, tecnologie e clienti.
- Attività di produzione di idrogeno verde.
- Gestione della sicurezza degli impianti e delle infrastrutture.
- Gestione dei rapporti con i dipendenti e i collaboratori.
- Attività di *marketing* e vendita di energia.
- Operazioni finanziarie e contabili.

I reati potenzialmente rilevanti ai sensi del dlgs 231/2001 includono:

- Reati contro la Pubblica Amministrazione (corruzione, concussione, abuso d'ufficio, traffico di influenze illecite).
- Reati societari (false comunicazioni sociali, aggio).
- Reati tributari (evasione fiscale, frode fiscale).
- Reati di riciclaggio e autoriciclaggio.
- Reati informatici (accesso abusivo a sistemi informatici, frode informatica).
- Reati transnazionali (corruzione di funzionari pubblici stranieri).

2.3 Mappatura dei rischi specifici

La Matrice dei Rischi (Allegato 3) identifica e valuta i rischi specifici associati a ciascuna area funzionale e attività a rischio, tenendo conto della probabilità e dell'impatto potenziale di ciascun reato.

La Matrice dei Rischi indica anche le misure di mitigazione adottate per ridurre la probabilità e l'impatto dei rischi identificati.

La Matrice dei Rischi è aggiornata periodicamente dall'OdV, in collaborazione con le aree funzionali competenti.

3. Principi generali di comportamento

3.1 Codice Etico

Il Codice Etico (Allegato 1) definisce i valori e i principi che guidano il comportamento di tutti i destinatari del Modello, tra cui:

- Integrità e onestà: agire sempre con correttezza, trasparenza e lealtà.

- Rispetto delle leggi e dei regolamenti: rispettare le leggi, i regolamenti e le procedure interne.
- Imparzialità e non discriminazione: evitare qualsiasi forma di discriminazione nei confronti di colleghi, clienti, fornitori e altri *stakeholder*.
- Rispetto dell'ambiente e della sicurezza: operare in modo sostenibile e sicuro, proteggendo l'ambiente e la salute dei lavoratori.
- Responsabilità sociale: contribuire al benessere della comunità e al progresso sociale.

Il Codice Etico è diffuso tra i destinatari attraverso la pubblicazione sul sito *web* aziendale, la distribuzione di copie digitali e la formazione specifica.

I dsoni tenuti a segnalare eventuali violazioni del Codice Etico attraverso il sistema di *whistleblowing*.

3.2 Principi di trasparenza e correttezza

Tutte le attività aziendali devono essere svolte con trasparenza e correttezza, evitando qualsiasi forma di opacità o ambiguità.

I rapporti con la Pubblica Amministrazione devono essere improntati alla massima trasparenza e correttezza, evitando qualsiasi forma di favoritismo o corruzione.

La selezione e la gestione dei fornitori devono essere basate su criteri oggettivi e trasparenti, evitando qualsiasi forma di conflitto di interesse.

3.3 Principi di diligenza e prudenza

I destinatari del Modello devono agire con diligenza e prudenza, valutando attentamente i rischi connessi alle proprie attività e adottando le misure necessarie per prevenirli o mitigarli.

In caso di dubbi o incertezze sull'interpretazione delle leggi o dei regolamenti, è necessario richiedere un parere legale o una consulenza specialistica.

È necessario segnalare tempestivamente eventuali anomalie o irregolarità riscontrate nello svolgimento delle proprie attività.

3.4 Conflitti di interesse

I Destinatari del Modello devono evitare qualsiasi situazione di conflitto di interesse, reale o potenziale, che possa compromettere la loro imparzialità e obiettività.

In caso di conflitto di interesse, è necessario informare tempestivamente il proprio superiore gerarchico e l'OdV, astenendosi dal prendere decisioni che possano favorire i propri interessi personali.

4. Sistema di controllo interno

4.1 Organismo di Vigilanza (OdV)

4.1.1 Composizione, nomina e durata in carica

L'OdV è un organo collegiale composto da tre membri, nominati dal Consiglio di Amministrazione. I membri dell'OdV devono possedere adeguate competenze in materia di diritto penale, diritto amministrativo, controllo interno e gestione dei rischi.

Salvo che il Consiglio di Amministrazione non decida di attribuire le funzioni di OdV al collegio sindacale, almeno un membro dell'OdV deve essere esterno alla Società, al fine di garantire l'indipendenza e l'obiettività dell'organo.

La durata in carica dei membri dell'OdV è di anni tre, rinnovabile.

La composizione e il funzionamento dell'OdV sono disciplinati dal Regolamento dell'Organismo di Vigilanza.

4.1.2 Poteri e responsabilità

L'OdV ha il compito di vigilare sull'efficace attuazione e sull'adeguatezza del Modello, monitorando le attività aziendali a rischio, ricevendo e gestendo le segnalazioni di violazioni

(*whistleblowing*), effettuando *audit* interni e controlli a campione, proponendo aggiornamenti al Modello e riferendo periodicamente al CdA sull'attività svolta.

L'OdV ha il potere di accedere a tutte le informazioni e i documenti necessari per svolgere il proprio lavoro, nonché di richiedere chiarimenti e spiegazioni ai Destinatari del Modello.

4.1.3 Flussi informativi verso l'OdV

Tutti i Destinatari del Modello sono tenuti a informare tempestivamente l'OdV di qualsiasi anomalia, irregolarità o violazione del Modello di cui vengano a conoscenza.

Le aree funzionali competenti sono tenute a fornire all'OdV informazioni periodiche sulle attività svolte e sui controlli effettuati.

L'OdV ha il potere di richiedere informazioni e documenti a tutte le aree funzionali della Società.

4.2 Funzioni di Controllo:

4.2.1 Internal Audit

La funzione di *Internal Audit* verifica l'efficacia del sistema di controllo interno e la conformità alle normative, effettuando audit periodici sulle diverse aree aziendali.

La funzione di *Internal Audit* riferisce direttamente all'OdV e al CdA.

4.2.2 Compliance

La funzione di *Compliance* assicura il rispetto delle leggi e dei regolamenti applicabili, monitorando l'evoluzione normativa e fornendo consulenza alle diverse aree aziendali.

La funzione di *Compliance* riferisce direttamente all'OdV e al CdA.

4.2.3 Risk Management

La funzione di *Risk Management* identifica e valuta i rischi aziendali e propone misure per mitigarli.

La funzione di *Risk Management* collabora con l'OdV per l'aggiornamento della Matrice dei Rischi (Allegato 3).

4.3 Sistema di deleghe e procure

La Società adotta un sistema di deleghe e procure che definisce chiaramente i poteri e le responsabilità dei diversi organi e funzioni aziendali.

Il sistema di deleghe e procure è documentato e aggiornato periodicamente.

Le deleghe e le procure devono essere rilasciate per iscritto e devono indicare i limiti dei poteri conferiti.

5. Aree Funzionali sensibili e protocolli

Introduzione:

Per ciascuna area funzionale considerata a rischio, sono definiti protocolli specifici volti a prevenire la commissione di reati.

I protocolli devono essere chiari, dettagliati, adattati alle specificità dell'area funzionale e aggiornati periodicamente.

5.1 Area Tecnica:

- Responsabilità: vigilanza sulla progettazione, costruzione e gestione dell'impianto di idrogeno verde. Controllo, per la parte tecnica, sulla rendicontazione fornita da terzi circa le spese e la loro ammissibilità ed eleggibilità, sostenute per l'attuazione del Progetto IPCEI. Procedure di gara e di negoziazione.
- Rischi Specifici: le numerose funzioni trasversali e, in particolare, quelle connesse alla scelta dei fornitori ed ai rapporti con i soggetti vigilati e/o controllati o verificati. fanno correre il rischio di reati contro la Pubblica Amministrazione, come il peculato e corruzione, le frode in pubbliche forniture, la truffa aggravata. Appare configurabile anche il rischio di concorrere nella realizzazione di reati tributari e societari, nel riciclaggio, auto riciclaggio di danaro e fattispecie similari, ed in quelli concernenti la sicurezza sui luoghi di lavoro.

5.1.1 Protocolli Specifici:

- **Attività di vigilanza tecnica:** protocollo dettagliato per lo svolgimento di tale attività, sia con riguardo agli adempimenti connessi per l'acquisizione delle aree che per la progettazione, costruzione e gestione dell'impianto di produzione di energia ad idrogeno verde, con checklist e procedure di controllo.
- **Gestione della Sicurezza:** protocollo per la gestione della sicurezza sul lavoro, con procedure di formazione, addestramento e controllo.
- **Attività di controllo:** per la parte e sugli aspetti tecnici della rendicontazione fornita da terzi circa le spese e la loro ammissibilità ed eleggibilità, sostenute per l'attuazione del Progetto IPCEI
- **Selezione fornitori:** protocollo per la selezione e qualifica dei fornitori, basato su criteri oggettivi e trasparenti, con verifica dell'integrità e dell'affidabilità dei fornitori.
- **Gestione dei rifiuti:** protocollo per la gestione dei rifiuti, con procedure di raccolta, stoccaggio, trasporto e smaltimento.

5.2 Area Comunicazione Istituzionale e Politica:

- Responsabilità: Relazioni con le istituzioni e la comunicazione esterna.
- Rischi Specifici: Traffico di influenze illecite, corruzione, finanziamento illecito di partiti politici.

5.2.1 Protocolli Specifici:

- **Gestione Rapporti con Istituzioni:** protocollo per la gestione dei rapporti con le istituzioni e i politici, improntato alla trasparenza e alla correttezza, con divieto di offrire o promettere vantaggi indebiti.
- **Sponsorizzazioni e Donazioni:** protocollo per la gestione delle sponsorizzazioni e delle donazioni, volto a garantire la loro liceità e trasparenza, con approvazione preventiva dell'OdV.
- **Attività di lobbying:** protocollo per la gestione delle attività di *lobbying*, con registrazione report delle comunicazioni e relazione sugli incontri con esponenti politici e istituzionali.

5.3 Area Relazioni Pubbliche e Internazionali:

- Responsabilità: Relazioni con *stakeholder*, media e organizzazioni internazionali.
- Rischi Specifici: Corruzione di funzionari pubblici stranieri, gestione opaca di donazioni e sponsorizzazioni.

5.3.1 Protocolli Specifici:

- **Due Diligence internazionale:** protocollo per la *due diligence* sui *partner* commerciali e sui consulenti internazionali, con verifica dell'integrità e dell'affidabilità.
- **Clausole contrattuali anticorruzione:** Protocollo per l'inserimento di clausole anticorruzione nei contratti con *partner* stranieri.
- **Formazione internazionale:** protocollo per la formazione specifica per il personale che opera all'estero sui rischi di corruzione.
- **Gestione donazioni internazionali:** protocollo per la gestione delle donazioni internazionali, garantendo la liceità e la trasparenza.

5.4 Area Amministrazione:

- Responsabilità: Gestione finanziaria, contabile e amministrativa. Gestione del personale. Acquisizione di beni e servizi necessari per le attività aziendali.

- Rischi Specifici: False comunicazioni sociali, utilizzo improprio di fondi pubblici, evasione fiscale, riciclaggio. Corruzione nella selezione dei fornitori, conflitto di interessi, frode negli appalti.

5.4.1 Protocolli Specifici:

- **Gestione flussi finanziari:** protocollo per la gestione dei flussi finanziari, volto a prevenire il riciclaggio di denaro, con separazione dei compiti tra chi autorizza le spese e chi le registra.
- **Controlli contabili:** protocollo per i controlli incrociati sui bilanci e sulle scritture contabili.
- **Gestione rapporti con l'Amministrazione Finanziaria:** protocollo per la gestione dei rapporti con l'Amministrazione Finanziaria, improntato alla correttezza e alla trasparenza.
- **Selezione e qualifica dei fornitori:** protocollo dettagliato per la selezione e qualifica dei fornitori, basato su criteri oggettivi e trasparenti, con verifica dell'integrità e dell'affidabilità dei fornitori.
- **Gestione degli appalti:** protocollo per la gestione degli appalti, con procedure di gara trasparenti e imparziali, e verifica della conformità alle normative applicabili.
- **Controllo dei prezzi:** protocollo per il controllo dei prezzi dei beni e dei servizi acquistati, con verifica della congruità e della competitività.
- **Gestione del personale:** protocollo volto a prevenire la commissione di reati contro la pubblica amministrazione attraverso idonea archiviazione e tracciabilità della documentazione inerente tale processo

6. Attività sensibili e protocolli

6.1. Gestione del personale.

6.1.1. I rischi reato. Il processo di amministrazione e gestione del personale potrebbe essere esposto al rischio di truffa ai danni dello Stato (art. 640, comma 2, n. 1, c.p.) qualora si procedesse alla mancata corresponsione degli oneri sociali dovuti mediante la falsificazione dei dati riguardanti il personale.

Trattasi, tuttavia, di rischio mappato in via prudenziale, risultando del tutto marginale, in simili casi, la contestazione di simile reato da parte delle Autorità procedenti, essendo di regola riportato da queste a fattispecie non inserito nel catalogo dei reati presupposto rilevanti agli effetti del dlgs 231/2001.

Più significativo è il rischio reato di frode informatica (Art.640 ter c.p.), astrattamente ipotizzabile mediante

l'inserimento di dati non veritieri in software di proprietà della PA per adempimenti previdenziali contributivi o inserimento di qualunque ulteriore dato.

6.1.2. Procedure e protocolli. E' attribuito in capo al Direttore Generale il potere di sovrintendere e coordinare le strutture deputate allo svolgimento delle attività di gestione del personale. Il Direttore Generale ha delegato interamente la funzione di controllo al responsabile dirigente dell'Area Amministrazione, il quale è tenuto a fornire periodicamente (almeno una volta ogni tre mesi) un *report* sull'andamento del controllo espletato sull'attività sensibile.

Viene, comunque, garantita una idonea archiviazione e tracciabilità della documentazione afferente all'attività in esame, sino alla determinazione delle poste da iscrivere in bilancio, tale da consentire la ricostruzione delle operazioni di contabilizzazione, in caso di verifiche *a posteriori*, nonché l'attuazione di idoneo protocollo operativo, atto a gestire il rischio reato, unitamente all'imposizione dell'obbligo di rispetto del Codice Etico e del Patto Tolleranza Zero Corruzione.

La Società, per l'elaborazione e la gestione del personale (es. ferie, legge 104, malattie) si avvarrà, ove occorra, di uno specifico *software*, assicurando comunque l'applicazione di idoneo sistema di rilevazione delle presenze.

6.2. Selezione e contrattualizzazione del personale e/o di professionisti.

6.2.1. I rischi reato. Il processo di selezione e contrattualizzazione del personale e/o di professionisti può essere strumentale rispetto alle varie fattispecie di reato di corruzione (art. 318 e ss. c.p.). Invero, l'assunzione o la contrattualizzazione potrebbe costituire "l'altra utilità" da riconoscere o, semplicemente, promettere, al Pubblico Ufficiale o all'incaricato di Pubblico Servizio, al fine di ricevere un vantaggio per la Società. Potrebbero anche essere configurate ipotesi di reato di corruzione tra privati (art. 2635 c.c.), in caso di rapporto instaurato con altro soggetto privato costituito in forma di società o di consorzio.

6.2.2. Procedure e protocolli. E' attribuito in capo al Direttore Generale il potere di assumere mere risorse interne e collaborazioni esterne nel rispetto della vigente normativa legale e contrattuale (ivi compresa quella dei Contratti Collettivi Nazionali di Lavoro) e delle direttive fornite dal Consiglio di Amministrazione, nell'ambito della pianta organica, ove approvata, e sulla base di opportune procedure selettive. Può essere favorito il ricorso ad agenzie interinali ed a forme di collaborazioni agili. La firma su qualsiasi contratto di lavoro e/o di collaborazione viene apposta dal Direttore Generale. La Società si avvarrà di idoneo protocollo operativo, e, in genere, di procedure trasparenti e chiare, al fine di gestire ed attenuare il rischio reato, unitamente all'imposizione dell'obbligo di rispetto del Codice Etico e del Patto Tolleranza Zero Corruzione.

6.3. Gestione delle procedure di gara o di negoziazione indette da enti pubblici nazionali o esteri per l'assegnazione di commesse, di concessioni, o per la erogazione di contributi o finanziamenti. Gestione dei relativi contratti e convenzioni. Gestione del processo di approvvigionamento di beni e servizi.

6.3.1. I rischi reato. L'attività che attiene alle gestione delle procedure di gara o di negoziazione indette da enti pubblici e quella di gestione dei relativi contratti e rapporti che si vengono ad instaurare, nonché l'attività diretta all'approvvigionamento di beni o servizi, potrebbe essere esposta al rischio di delitti contro la Pubblica Amministrazione, come corruzione, turbativa d'asta, frode nelle pubbliche forniture, truffa aggravata ai danno dello Stato e di enti pubblici. Ad esempio, l'acquisizione di forniture di beni o servizi totalmente o parzialmente inesistenti potrebbe essere effettuata al solo fine di costituire c.d. "riserve occulte" da utilizzare per attuare condotte corruttive nei confronti dei funzionari pubblici. Tali attività potrebbero anche dar luogo al rischio di reati di ricettazione, riciclaggio o impiego di denaro, beni o altra utilità di provenienza illecita, nonché a quello di corruzione tra privati.

6.3.2. Procedure e protocolli.

6.3.2.1. Ambito. Trattasi di attività sensibile che coinvolge tutte le Aree Funzionali. Nella misura in cui una determinata Area Funzionale sia coinvolta in un procedura di gara o di negoziazione o nella gestione del relativo contratto o convenzione, oppure ancora in una procedura di approvvigionamento di beni o servizi, è attribuito al Responsabile della stessa il compito di riportare, in una scheda dettagliata, gli adempimenti all'uopo eseguiti, assicurando agli stessi massima trasparenza, tracciabilità e verificabilità. Analogamente, tale Responsabile dovrà effettuare i riscontri del caso, e riferire al Direttore Generale l'esito degli stessi e la presenza e rilevanza di eventuali interferenze con le attività di altra Area Funzionale, in modo che venga assicurato il coordinamento degli interventi di spettanza di ciascuna di esse.

Il rischio potenziale concerne la possibilità di stipulare contratti per l'acquisto di beni o servizi derivanti da attività illecite, non accertandosi dell'attendibilità del fornitore, ovvero di effettuare pagamenti impropri per riciclare denaro proveniente da attività illecite.

In ogni caso, è stato ricordato che nel corso di una trattativa, richiesta o rapporto commerciale con la Pubblica Amministrazione è imposto il divieto di intraprendere, direttamente o indirettamente, le seguenti azioni:

- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione a titolo personale;
- offrire o in alcun modo fornire omaggi anche sotto forma di promozioni aziendali riservate ai soli dipendenti o attraverso ad esempio il pagamento di spese viaggi;
- sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti

Tutta la documentazione dovrà essere adeguatamente archiviata e conservata, per consentire la ricostruzione delle operazioni compiute, in caso di verifiche *a posteriori*.

Ciascuna Area dovrà munirsi di idoneo protocollo operativo, atto a gestire il rischio reato, nel rispetto del Codice Etico e del Patto Tolleranza Zero Corruzione.

Nei rapporti con i terzi a ciascuna Area sono state impartite le seguenti disposizioni:

6.3.2.2. Selezione e qualifica dei fornitori:

- Adozione di criteri oggettivi e trasparenti per la selezione dei fornitori, basati sulla qualità, il prezzo, l'affidabilità e l'integrità.
- Verifica della reputazione e dell'affidabilità dei fornitori, attraverso la consultazione di banche dati, visure camerali e referenze commerciali.
- Richiesta di certificazioni e attestazioni di conformità alle normative applicabili (es. certificazioni ambientali, di sicurezza, di qualità).

6.3.2.3. Contratti e clausole risolutive:

- Inserimento nei contratti con i fornitori clausole risolutive espresse in caso di violazioni del Codice Etico o del Modello.
- Previsione di penali per inadempimenti contrattuali.
- Diritto di recesso dal contratto in caso di condotte illecite da parte del fornitore.
- Clausole che prevedano la possibilità di effettuare *audit* e controlli presso i fornitori.

6.3.2.4. Due diligence:

- Effettuazione di *due diligence* sui *partner* commerciali e sui consulenti, al fine di verificare la loro integrità e affidabilità, in particolare per i rapporti con soggetti operanti in paesi a rischio di corruzione.
- La *due diligence* deve includere la verifica della reputazione, della storia aziendale, della conformità alle normative e della presenza di eventuali conflitti di interesse.

6.4. Gestione delle attività di pubbliche relazioni

6.4.1. I rischi reato. Nell'attività riguardante le relazioni istituzionali con Enti pubblici (Ministeri, Regioni, Comuni, Autorità Pubbliche in genere, funzionari europei) potrebbe astrattamente configurarsi il rischio di reati contro la Pubblica Amministrazione al fine di influenzare i Pubblici Ufficiali o gli Incaricati di Pubblico Servizio per la definizione favorevole di una pratica amministrativa *in itinere*.

6.4.2. Procedure e protocolli. E' stato demandato ai Responsabili delle Aree Funzionali della Comunicazione Istituzionale e Politica e delle Relazioni Pubbliche e Internazionali, di assumere, in raccordo tra loro e informando il Direttore Generale, ogni iniziativa organizzativa affinché vengano effettuate comunicazioni, istanze, richieste di autorizzazione e quant'altro necessario ai fini del corretto e puntuale espletamento degli adempimenti propri delle proprie Aree, nel pieno rispetto dalle disposizioni normative e regolamentari, e dei principi di trasparenza, chiarezza e proporzionalità. Ove occorra, viene suggerito di esternalizzare parte delle funzioni a soggetto idoneo. In ogni caso, è stato ricordato che nel corso di una trattativa, richiesta o rapporto

commerciale con la Pubblica Amministrazione è imposto il divieto di intraprendere, direttamente o indirettamente, le seguenti azioni:

- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione a titolo personale;
- offrire o in alcun modo fornire omaggi anche sotto forma di promozioni aziendali riservate ai soli dipendenti o attraverso ad esempio il pagamento di spese viaggi;
- sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti

Ciascuna Area coinvolta in tale rischio – reato, dovrà comunque operare nel rispetto del Codice Etico e del Patto Tolleranza Zero Corruzione.

6.5. Gestione dei sistemi informatici

6.5.1. I rischi reato. Nel corso delle attività della Società, potrebbero essere commessi reati informatici e illecito trattamento dei dati. Si considera delitto informatico tanto la frode commessa attraverso il computer che il danneggiamento o l'accesso abusivo ad un sistema informatico o telematico. Tali reati potrebbero essere integrati con l'introduzione, senza autorizzazione, in sistemi protetti da misure di sicurezza; attraverso il possesso abusivo di codici o altri mezzi di accesso ad un sistema informatico protetto; con la diffusione di programmi idonei a danneggiare un sistema informatico di un terzo; con l'intercettazione abusiva di una conversazione informatica; attraverso la distruzione, il deterioramento o la cancellazione di informazioni, dati o programmi informatici. Il reato di falsità in documenti informatici, invece, potrebbe essere realizzato dai soggetti di volta in volta interessati attraverso, ad esempio, la falsa attestazione, in atti e documenti informatici, di fatti dei quali l'atto o il documento stesso è destinato a provare la veridicità.

6.5.2. Procedure e protocolli. La Società ha demandato a soggetto esterno la gestione della sicurezza dei propri sistemi informatici e la relativa responsabilità. Esiste e viene mantenuto un inventario aggiornato delle applicazioni e delle banche dati di pertinenza della Società.

L'accesso alle applicazioni aziendali è consentito solo tramite credenziali di autenticazione (*user-id* e *password*). I sistemi tracciano anche gli accessi degli utenti esterni alla rete, sia se operati con successo sia se falliti. In tal modo, si assicura la tracciatura degli accessi degli utenti alla rete, alle transazioni, ai sistemi ed agli applicativi. Viene applicato il principio di separazione dei compiti per ridurre il rischio di modifiche non autorizzate o utilizzo improprio delle informazioni. Sono stabiliti inoltre e formalizzati controlli di sicurezza nei contratti con terze parti per *l'outsourcing* di attività di elaborazione. E' installato e regolarmente aggiornato un software anti-virus su tutti i server e client. Sono verificati gli allegati di posta elettronica e i download da Internet. Vengono adottate procedure per il ripristino dei sistemi in caso di emergenza da virus. Vengono effettuate attività periodiche di verifica del software installato. La Società ha adottato e comunicato una *policy* sul corretto utilizzo della posta elettronica e sono stati analizzati i possibili rischi di sicurezza connessi all'utilizzo della stessa. Sono adottati meccanismi di sicurezza delle informazioni scambiate e anche adottata una procedura per la conservazione e l'archiviazione delle stesse.

La Società ha adottato controlli per assicurare che l'imputazione dei dati sia corretta ed appropriata, per rilevare errori nella elaborazione dei dati, per verificare l'autenticità del contenuto delle transazioni elettroniche e la correttezza dei dati di *output*.

Sono definite responsabilità e procedure per la risposta ed incidenti relativi alla sicurezza logica delle infrastrutture informatiche. Sono utilizzate tecniche specifiche di crittografia per la protezione di informazioni critiche. Sono infine utilizzati documenti informatici firmati digitalmente all'interno dei processi aziendali.

Viene effettuata un'attività di formazione periodica dei dipendenti sulle tematiche *privacy* e sulla sicurezza delle informazioni.

6.6. Gestione finanziaria e contabile. Attività di formazione e approvazione del bilancio.

6.6.1. I rischi reato. Tale attività, che prospetta il rischio di reati societari, comprende la raccolta, aggregazione e valutazione dei dati contabili volte alla predisposizione dei bilanci annuali, situazioni economiche, finanziarie e patrimoniali; definizione delle poste valutative di bilancio.

I reati indicati potrebbero essere realizzati mediante l'esposizione di dati contabili non rispondenti al vero anche attraverso la variazione dei conti esistenti, l'inserimento di poste a valori difformi da quelle reali (come, ad esempio, la sopravvalutazione dei crediti, etc.), l'occultamento di risorse aziendali in fondi liquidi o riserve occulte.

Ai fini dei reati societari assumono rilievo anche le attività di inserimento, variazione o cancellazione dei dati rilevanti ai fini della contabilità generale nel *software* gestionale o nel sistema informatico di supporto. Il rischio di commissione dei reati di cui trattasi è ipotizzabile tenuto conto che attraverso i processi amministrativo-contabili si giunge alla formazione del dato contabile destinato a confluire nei bilanci, nelle relazioni e nelle situazioni patrimoniali richieste dalla legge.

La veridicità dei dati potrebbe, pertanto, essere inficiata in una fase precedente rispetto alla formazione del bilancio.

6.6.2. Procedure e protocolli. La società si avvale di un gestionale interno per la fatturazione attiva, mentre la contabilità è tenuta da studio professionale esterno, attraverso un proprio sistema specifico. Tale attività, con riguardo ai progetti finanziati sottoposti a rendicontazione o a contabilità separata, è agevolata dalla apertura di conti correnti bancari dedicati. Tali attività fanno capo all'Area Amministrazione, all'interno della quale esiste una separazione di funzioni tra chi emette gli ordini, riceve le forniture di beni e servizi, contabilizza gli acquisti ed effettua i pagamenti. Per le attività di cui trattasi, il responsabile dell'Area Amministrazione è tenuto a raccordarsi ed a riferire al Direttore Generale.

6.7. Gestione dei fondi pubblici e rendicontazione.

6.7.1. I rischi reato. Trattasi di attività sensibile a rischio reati contro la pubblica amministrazione, a partire da peculato e corruzione, frodi e truffa ai danni dello Stato e per il conseguimento di erogazioni pubbliche, reati di riciclaggio, reati societari.

Sono coinvolte in tale attività, tutte le Aree Funzionali sopra indicate, ciascuna per la parte di propria competenza. Tutti i soggetti appartenente a tali Aree, pertanto, saranno tenuti a conoscere, a rispettare ed a verificare che vengano rispettate le disposizioni dettate in merito a tale ambito. A tal fine, si indicano qui di seguito i punti significativi per assicurare il rispetto delle regole.

6.7.2. Procedure e protocolli. Sono stati configurati e definiti i seguenti interventi:

6.7.2.1. Procedure per l'utilizzo dei Fondi:

- Definizione chiara degli obiettivi e delle modalità di utilizzo dei fondi pubblici, in conformità ai bandi e alle normative.
- Tracciabilità di tutte le operazioni finanziarie relative ai fondi pubblici, con registrazione dettagliata di tutte le entrate e le uscite.
- Separazione dei conti correnti dedicati ai fondi pubblici da quelli utilizzati per le attività ordinarie della Società.
- Autorizzazione preventiva di tutte le spese da parte di un responsabile designato, con verifica della conformità agli obiettivi e alle modalità di utilizzo dei fondi.

6.7.2.2. Controlli sulla rendicontazione:

- Verifica della conformità delle spese ai criteri stabiliti dalle normative e dai bandi di finanziamento, con raccolta e conservazione di tutta la documentazione giustificativa.
- Revisione indipendente della rendicontazione prima della sua presentazione all'ente erogatore, con verifica della completezza e dell'accuratezza dei dati.

- Formazione specifica per il personale addetto alla rendicontazione, con aggiornamento continuo sulle normative e le procedure.

6.7.2.3. Tracciabilità dei pagamenti:

- Utilizzo esclusivo di bonifici bancari o altri mezzi di pagamento tracciabili per i pagamenti superiori a una certa soglia.
- Indicazione chiara della causale del pagamento in tutti i documenti contabili, con riferimento al progetto o all'attività finanziata con i fondi pubblici.
- Conservazione di tutte le ricevute e fatture relative ai pagamenti, con verifica della conformità alle normative fiscali.

6.7.2.4. Rapporti con gli enti erogatori:

- Gestione dei rapporti con gli enti erogatori in modo trasparente e corretto, fornendo tutte le informazioni e la documentazione richieste.
- Risposta tempestiva alle richieste di chiarimenti o integrazioni da parte degli enti erogatori.
- Segnalazione immediata all'OdV di eventuali anomalie o irregolarità riscontrate nella gestione dei fondi pubblici.

7. Sistema disciplinare

7.1 Sanzioni per violazioni del Modello:

Il sistema disciplinare prevede sanzioni proporzionate alla gravità della violazione, che possono andare dal richiamo verbale alla sospensione dal lavoro fino al licenziamento, a seconda della gravità della violazione e delle circostanze specifiche del caso.

Le sanzioni sono applicate nel rispetto delle disposizioni del Contratto Collettivo Nazionale di Lavoro (CCNL) e delle leggi vigenti.

Le violazioni del Modello che possono comportare sanzioni disciplinari includono, a titolo esemplificativo:

- Violazioni del Codice Etico.
- Violazioni delle procedure interne.
- Commissione di reati.
- Omissione di segnalazione di illeciti.
- Ritorsioni nei confronti dei segnalanti (*whistleblowers*).

7.2 Whistleblowing:

La Società Energie Salentine S.p.A. istituisce un sistema di *whistleblowing* per consentire ai destinatari del Modello di segnalare in modo confidenziale eventuali illeciti o violazioni di cui vengano a conoscenza.

Il sistema di *whistleblowing* è gestito dall'OdV, che garantisce la riservatezza delle segnalazioni e la protezione dei segnalanti da eventuali ritorsioni.

Le segnalazioni possono essere effettuate per iscritto o verbalmente, anche in forma anonima.

L'OdV si impegna a esaminare tempestivamente e accuratamente tutte le segnalazioni ricevute, adottando le misure necessarie per accertare i fatti e adottare eventuali azioni correttive.

È vietata qualsiasi forma di ritorsione nei confronti dei segnalanti.

8. Formazione e informazione

8.1 Programmi di formazione:

La Società organizza programmi di formazione specifici per i destinatari del Modello, al fine di sensibilizzarli sui rischi di reato e di promuovere una cultura aziendale improntata all'etica e alla legalità.

La formazione è differenziata in base al ruolo e alle responsabilità dei destinatari.

I programmi di formazione includono:

- Formazione iniziale per i nuovi assunti.
- Formazione periodica di aggiornamento per tutti i destinatari.
- Formazione specifica per i soggetti che operano in aree a rischio.

La formazione è erogata attraverso corsi in aula, e-learning, seminari e materiale informativo.

8.2 Diffusione del Modello:

Il Modello è messo a disposizione di tutti i destinatari, anche attraverso la pubblicazione sul sito web aziendale e l'invio, a richiesta, di copie cartacee.

La Società si impegna a diffondere il Modello tra i propri *partner* commerciali e fornitori, ed a chiederne il rispetto

9. Monitoraggio e aggiornamento del Modello

9.1 Attività di monitoraggio dell'OdV:

L'OdV monitora continuamente l'attuazione del Modello e l'efficacia delle misure di prevenzione dei reati, attraverso:

- Analisi dei flussi informativi.
- Verifica del rispetto delle procedure interne.
- Effettuazione di *audit* interni e controlli a campione.
- Gestione delle segnalazioni di violazioni (*whistleblowing*).
- Partecipazione a riunioni con le aree funzionali competenti.

L'OdV redige un rapporto periodico sull'attività svolta, da presentare al CdA.

9.2 Revisione e aggiornamento del Modello:

Il Modello è rivisto periodicamente (almeno annualmente) e in caso di modifiche normative, cambiamenti nella struttura aziendale o nuove aree di rischio.

L'OdV è responsabile della revisione e dell'aggiornamento del Modello, in collaborazione con il CdA e le aree funzionali competenti.

Le modifiche al Modello sono approvate dal CdA e comunicate a tutti i Destinatari.

Allegati

- Allegato 1: Codice Etico
- Allegato 2: Organigramma Societario
- Allegato 3: Matrice dei Rischi