

MODELLO DI ORGANIZZAZIONE E DI GESTIONE AZIENDALE

ai sensi dell'ex D.Lgs. 231/01 e s.m.i.

di



S.I.O.S.S. INFRASTRUTTURE S.r.l.

Via dell'industria, 14/16 – 34077 Ronchi dei Legionari (GO)

P.Iva 03192280307



Versione attuale

Revisione 02 del 02.02.2026

- Cambio ragione sociale, proprietà e passaggio da Cda ad Amministratore Unico

Approvato dall'Amministratore Unico

Sig. Puntin Maurizio

Firma

Tabella delle revisioni

Rev. 00 – 22.03.2021	Prima Emissione
Rev. 01 – 10.12.2024	Aggiornamento Whistleblowing (cfr. D.lgs. 24/2023) Aggiornamento reati fino alla L.n. 166 del 14.11.2024
Revisione	Note alla revisione

MODELLO DI ORGANIZZAZIONE E DI GESTIONE AZIENDALE

Sommario

1.	PREMESSA	4
2.	DESCRIZIONE DELL'AZIENDA	5
3.	RISORSE UMANE	8
3.1	Generalità	8
3.2	Competenza, consapevolezza ed addestramento	8
4.	IL M.O.G.: CARATTERISTICHE, OBIETTIVI E FINALITÀ	9
5.	ATTIVITÀ SVOLTE PER LA PREDISPOSIZIONE DEL MODELLO: LE 5 FASI	11
5.1	Fasi dell'intervento	12
6.	DESTINATARI DEL MODELLO	12
7.	ORGANISMO DI VIGILANZA (O.d.V.)	13
7.1	Identificazione, nomina e requisiti dell'Organismo di Vigilanza	13
7.2	Cause di ineleggibilità dell'Organismo di Vigilanza	14
7.3	Funzioni e poteri dell'Organismo di Vigilanza	14
7.4	Aggiornamento del Modello	16
7.5	Compiti specifici	16
7.6	Flussi informativi dall'Organismo di Vigilanza	17
7.7	Flussi informativi nei confronti dell'Organismo di Vigilanza	18
8.	IL SISTEMA DI DELEGHE E PROCURE	19
9.	MODALITÀ DI GESTIONE DELLE RISORSE FINANZIARIE	20
10.	CODICE ETICO	21
11.	INFORMAZIONE, FORMAZIONE E COMUNICAZIONE	21
12.	SISTEMA DISCIPLINARE	22
	PARTE SPECIALE	22
1.	PREMESSA	22
2.	PROTOCOLLI DI PREVENZIONE E SISTEMA DEI CONTROLLI	22
3.	PROTOCOLLI GENERALI	23
3.1.	Norme comportamentali e codici di condotta	23
3.2.	Poteri autorizzativi e di firma	23
3.3.	Procedure e norme interne	23
3.5.	Documentabilità e Tracciabilità	24
4.	PROTOCOLLI SPECIFICI DI PROCESSO	24
4.1.	Gestione del fabbisogno e degli acquisti	25
4.1.	Protocollo Risorse Umane	28
4.2.	Protocollo Informatico	31
4.3.	Protocollo Amministrativo	36
4.4.	Protocollo pubblica amministrazione	40
4.5.	Protocollo anticorruzione	44
4.6.	Gestione degli aspetti ambientali	47
4.7.	Gestione della Salute e Sicurezza sui Luoghi di Lavoro	50
5.	ORGANISMO DI VIGILANZA (OdV)	52
6.	CODICE ETICO	52
7.	SISTEMA SANZIONATORIO	52
8.	RIESAME DEL SISTEMA	52
9.	RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI	52

1. PREMESSA

Sulla base del Decreto Legislativo 231 del 2001, le aziende e gli enti in genere possono essere chiamati a rispondere in sede penale per taluni reati commessi nel proprio interesse o vantaggio dagli amministratori o dai dipendenti che ivi prestano servizio. Con l'espressione "il 231" si fa riferimento al quadro normativo che disciplina la responsabilità diretta delle aziende di fronte all'emersione di varie tipologie di reato.

Pertanto, conscio dell'inadeguatezza dell'azione pubblica di contrasto del crescente fenomeno della criminalità d'impresa, il Legislatore ha ritenuto di voler coinvolgere direttamente gli operatori economici, sollecitandoli ad una efficace azione di prevenzione all'interno delle proprie realtà aziendali, pena la loro responsabilità diretta ove, a causa della loro negligenza, si sia realizzato un reato. Ne risulta una nuova cultura aziendale, una moderna modalità di fare impresa conformemente ai principi dell'etica e della trasparenza. L'azienda che si sia uniformata al D.Lgs. 231 e s.m.i. dotandosi, volontariamente, di efficaci strumenti di prevenzione dei reati, oltre al possibile beneficio pratico, acquista anche una patente di "impresa d.o.c.", un nuovo "marchio di qualità" capace di dare una peculiare connotazione all'azienda, favorendola nel confronto con la concorrenza sul mercato, specie internazionale ed oggi globale.

Il Decreto Legislativo 231/2001

Il **D.Lgs. 08.06.2001 n. 231** ha introdotto, per la prima volta nel nostro ordinamento, la previsione di una responsabilità personale e diretta dell'azienda in quanto soggetto collettivo (azienda privata, associazione riconosciuta e non, azienda pubblica) per la commissione di una serie di reati da parte delle persone fisiche ad esso legate, che abbiano agito nell'interesse o a vantaggio dell'azienda.

La *ratio* della legge che si conforma a normative e convenzioni internazionali in materia di lotta alla criminalità d'impresa, è quella di sensibilizzare gli enti alla prevenzione dei reati economici o contro le persone, sancendo la loro "responsabilità personale" per il caso di omissione o negligenza.

L'azienda risponde personalmente del reato realizzato, rispettivamente da:

- Persone operanti in "posizione apicale" (responsabili di funzione);
- Lavoratori dipendenti (lavoratore subordinato od equiparato).

L'azienda promuove una sensibilizzazione verso le tematiche del D.lgs 231/01 anche nei confronti dei fornitori e/o collaboratori a diverso titolo.

L'assunzione ed implementazione preventiva di Codici Etici e comportamentali, e di programmazione dell'attività decisionale in specifiche aree e funzioni aziendali, oltre all'attivazione di un **Organismo di Vigilanza**, autonomo ed indipendente, favoriscono comportamenti virtuosi, i quali, contribuendo alla prevenzione dei vari reati, se assunti congruamente e *in toto* dalla società, sono ritenuti dal giudice penale idonei ad escludere la sua (della società/azienda) responsabilità diretta per i reati stessi (condizione esimente).

L'adozione di tali strumenti di analisi e prevenzione, richiede un'attività di rilevazione ed elaborazione di dati e documenti, come di seguito indicato:

- la determinazione dei principi etici cui l'azienda intende uniformarsi (Codice Etico), la mappatura delle singole aree aziendali esposte al rischio che siano commessi i reati previsti dal D.Lgs. 231/2001 e s.m.i.;

- l'elaborazione di modelli comportamentali e gestionali atti a generare una sensibilità ed una cultura capace di favorire degli standard e delle procedure positive in tutti coloro che operano negli ambiti e nelle funzioni "a rischio";¹
- l'istituzione dell'Organismo di Vigilanza, deputato a monitorare l'applicazione, la conformazione e l'adeguamento dei Modelli assunti, nonché l'applicazione di un sistema correttivo e, se del caso, sanzionatorio per le violazioni realizzate.

L'adozione di congrui modelli si rende necessaria per scongiurare i vari reati, connessi a processi decisionali realizzati in tutti gli ambiti aziendali, come ad esempio: nel trattamento e nella gestione del personale, nell'aggiudicazione di gare di pubblico appalto; nei rapporti con la P.A.; nell'ottenimento di autorizzazioni, licenze, concessioni, finanziamenti; nella commissione di reati penali di natura societaria (violazione di obblighi degli organi ed operazioni sul capitale); nella irregolare gestione finanziaria e nella frode informatica, nei reati ambientali e reati in materia di tutela della sicurezza e salute dei lavoratori.

Il D.Lgs 231/2001 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.²

In particolare, a norma dell'art. 5 del D.Lgs 231/2001 l'azienda risponde per i reati commessi nel suo interesse ed a suo vantaggio da:

- a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'azienda 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 (soggetti in posizione apicale);
- b) lavoratori dipendenti (lavoratore subordinato od equiparato), collaboratori a diverso titolo.³

2. DESCRIZIONE DELL'AZIENDA

S.I.O.S.S. Infrastrutture S.r.l. (di seguito S.I.O.S.S. o Azienda) è stata costituita ad ottobre 2025 con inizio attività dal 21.01.2026. Questa società è nata grazie alla cessione del ramo d'azienda da parte di S.I.O.S.S. – Società Italiana Operatori Segnaletica Stradale S.r.l.. Tale processo che ha consentito il trasferimento automatico di tutti i requisiti e le certificazioni possedute alla **S.I.O.S.S. Infrastrutture S.r.l.**

La manutenzione è l'attività cardine dell'azienda, nonché elemento fondamentale per la conservazione in efficienza dell'infrastruttura (auto) stradale. I settori d'intervento sono molteplici: riguardano la manutenzione del piano viabile, in termini di interventi preventivi e correttivi della regolarità ed aderenza della pavimentazione, della segnaletica orizzontale e verticale, di installazione di barriere fonoassorbenti e paramassi, del sicurvia metallico di protezione nonché il mantenimento della funzionalità dei sistemi protezione con la riparazione tempestiva di tutte le opere danneggiate da incidenti.

¹ Distinguendo tra: a) figure apicali e di responsabilità, e b) personale operativo subordinato.

² Si deve ricordare che la responsabilità dell'azienda può sussistere solo per i reati tassativamente indicati nel D.Lgs 231/2001 e s.m.i. e si aggiunge alla responsabilità penale dell'autore del reato.

³ In nessun caso l'azienda risponde se chi ha commesso il reato ha agito esclusivamente nel proprio interesse e vantaggio.

Essendo un'impresa di medie dimensioni e avendo acquisito know how tecnico garantito dall'elevata specializzazione del personale e dalla disponibilità di attrezzature fra le più moderne, la **S.I.O.S.S.** è in grado di eseguire qualsiasi lavoro di segnaletica orizzontale, verticale, barriere di sicurezza, reti di recinzione, di barriere fonoassorbenti e paramassi ed interventi per la sicurezza del traffico sia su strade ordinarie che su autostrade. Tra i principali committenti si possono annoverare: Autostrade per l'Italia S.p.A., Autostrada del Brennero S.p.A., Autovie Venete S.p.A., Società Autostrada Tirrenica p.A., Autostrada Brescia Verona Vicenza Padova S.p.A., Concessioni Autostradali Venete S.p.A. ANAS S.p.A. Compartimento vari – Friuli Venezia Giulia Strade S.p.A., Provincie e Comune vari.

La **S.I.O.S.S.** ha la disponibilità di uno staff tecnico che le consente di effettuare progettazioni e di proporre soluzioni tecniche che le derivano dall'esperienza conseguita negli anni e dalla conoscenza delle tecniche più avanzate adottate in Italia ed in altri paesi europei.

La Ditta possiede le più moderne attrezzature e macchinari disponibili sul mercato per l'esecuzione della segnaletica orizzontale in materiale termoplastico, vernice acrilica e vernice all'acqua. Trattasi di macchinari semoventi con gruppi di spruzzatura doppia, che consentono un'elevata potenzialità di applicazione giornaliera permettendo di diminuire notevolmente il costo della manodopera impiegata.

Le squadre operative sono composte da personale specializzato che esegue lavori di segnaletica stradale su tutto il territorio nazionale. Il lavoro delle squadre è coadiuvato da un ufficio tecnico attrezzato che offre anche un servizio di studio, pianificazione e che mette a disposizione una lunga esperienza per la ricerca di valide soluzioni ai problemi della viabilità.

La segnaletica orizzontale è un elemento fondamentale per la sicurezza e nel corso dell'anno, con attrezzature appositamente studiate, vengono effettuati controlli sistematici delle caratteristiche di rifrangenza della segnaletica orizzontale ed al calare dei parametri di riferimento si provvede a ripristinare l'efficienza delle stesse, effettuando i necessari ripassi.

La struttura tecnica interna è organizzata in modo tale da compiere, quotidianamente, ispezioni, ripristini e manutenzioni per mantenere sempre in piena efficienza i tratti autostradali appaltati.

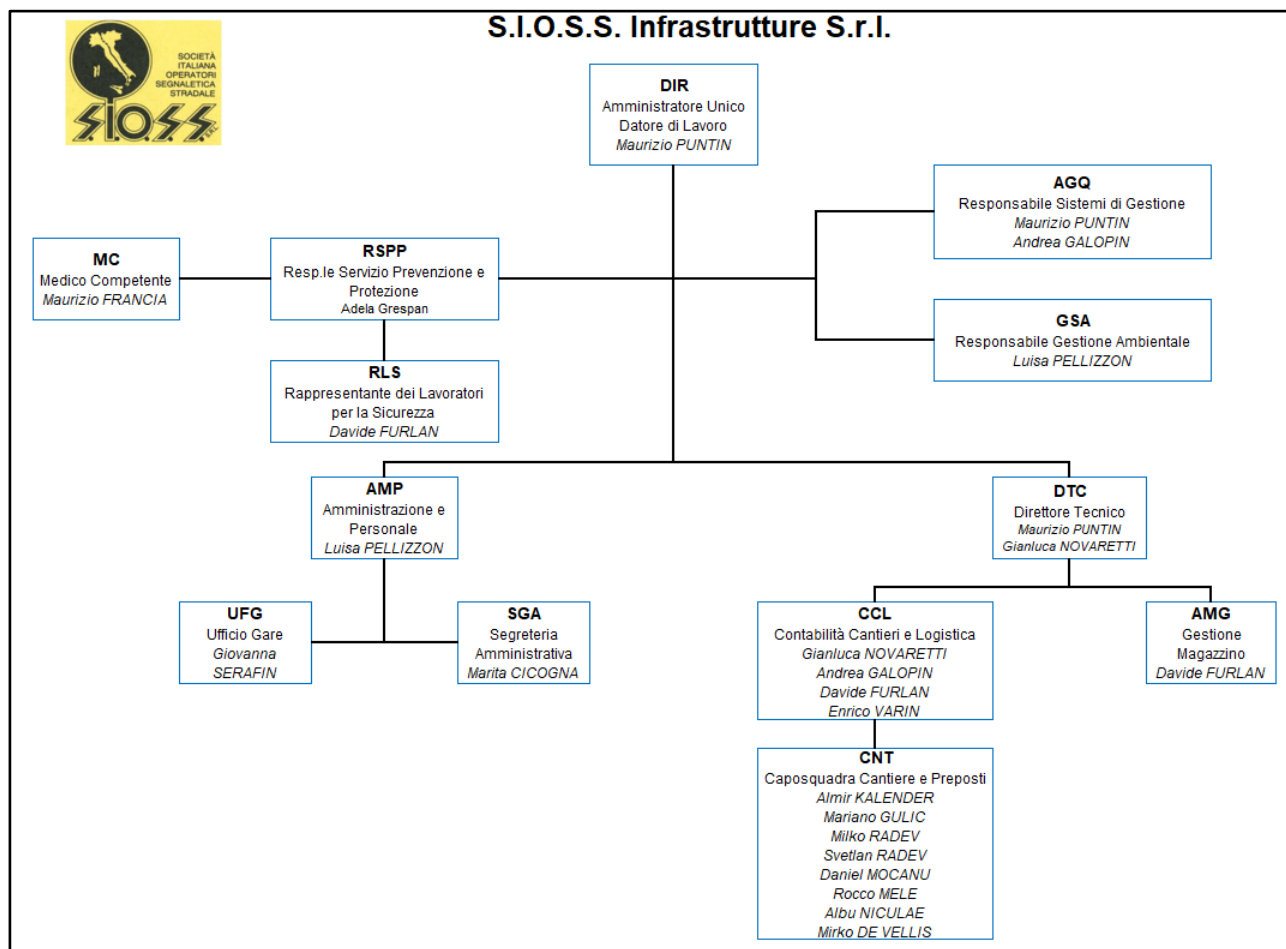
S.I.O.S.S. opera in due insediamenti di proprietà di S.I.O.S.S. – Società Italiana Operatori Segnaletica Stradale S.r.l. che si sviluppano su un'area di 6.250,00 mq ubicati nella zona artigianale di Ronchi dei Legionari (GO), dove si trovano i magazzini, il ricovero attrezzi, attrezzature e macchinari oltre ad un'officina per le piccole manutenzioni e riparazioni degli stessi.

L'attività di cui sopra avviene su tutto il territorio nazionale.

S.I.O.S.S. Infrastrutture è una Società a Responsabilità Limitata il cui unico socio è **S.I.O.S.S. – Società Italiana Operatori Segnaletica Stradale S.r.l.**

L'azienda è gestita da un amministratore Unico - Sig. Puntin Maurizio

Segue l'organigramma funzionale e nominativo dell'azienda:

MODELLO DI ORGANIZZAZIONE E DI GESTIONE AZIENDALE


Certificazioni

Le certificazioni che seguono sono state trasferite grazie alla cessione del ramo d'azienda.

Per garantire la qualità del servizio vengono adoperati prodotti selezionati realizzati secondo processi produttivi all'avanguardia e in possesso della certificazione ISO 9001.

La **S.I.O.S.S.**, ha ottenuto la certificazione ISO 9001 nell'anno 1998, nell'anno 2000 la Vision 2000 e nell'anno 2017 la **ISO 9001:2015**.

Nell'anno 2015 ha conseguito la certificazione n. OHS -2384 che certifica che il Sistema di Gestione della Sicurezza e della Salute sul luogo di lavoro applicato dalla S.I.O.S.S. S.r.l. è conforme alla norma **OHSAS 18001:2007** e nel 2020 il medesimo sistema è stato adeguato alla **ISO 45001:2018** (certificato n. OHS-2384).

Nell'anno 2016 ha conseguito la certificazione n. EMS – 6578/S che certifica che il Sistema di Gestione Ambientale applicato dalla **S.I.O.S.S.** è conforme alla norma **ISO 14001:2015**.

Nell'anno 2017 ha conseguito la certificazione n. RTS 18/17/S che certifica che il Sistema di Gestione della Sicurezza stradale applicato dalla S.I.O.S.S. è conforme alla norma **ISO 39001:2018** (Road Traffic Safety RTS Management System).

Inoltre ha diverse attestazioni SOA per le seguenti categorie:

Categoria	Descrizione	Importo (Euro)	Classifica
OS 10	Segnaletica stradale non luminosa	Illimitata	VIII
OS 11	Apparecchiature strutturali speciali	258.000,00	I
OS 12 A	Barriere stradali di Sicurezza	5.165.000,00	V
OS 12 B	Barriere parasassi, fermaneve e simili	2.582.000,00	IV
OG 3	Strade, autostrade, ponti, viadotti, ferrovie, metropolitane	1.500.000,00	III-bis
OS 34	Sistemi antirumore per infrastrutture di mobilità	1.033.000,00	III

3. RISORSE UMANE

3.1 Generalità

La competenza e il costante aggiornamento dei propri addetti è considerato dall'Azienda un elemento strategico fondamentale. La Direzione aziendale dispone che il personale sia sempre in linea con lo stato dell'arte nel proprio settore tramite una sistematica verifica della sua competenza.

La Direzione aziendale definisce per ciascuna mansione tipica dell'area di impiego, un "livello di competenza". Tale livello è definito sulla base degli elementi posseduti dall'addetto, il suo grado di istruzione, corsi di aggiornamento cui ha partecipato, esperienze di lavoro nell'Azienda o in altre, lavori di prova. Il Responsabile della suddetta valutazione può derogare da un elemento (ad esempio un diploma scolastico) quando vi sia l'evidenza che l'addetto ha ottenuto il medesimo livello di preparazione in altro modo (ad esempio con l'esperienza lavorativa).

3.2 Competenza, consapevolezza ed addestramento

Per quanto riguarda la competenza, la Direzione, tenendo nella dovuta considerazione gli esiti riscontrati nei diversi processi aziendali, individua le competenze minime necessarie (incluse quelle previste dalle normative cogenti) degli addetti impegnati in quelle attività che impattano sulla qualità dei servizi.

Per quanto riguarda la consapevolezza, la Direzione si preoccupa di informare e aggiornare gli addetti sulla rilevanza della loro attività nel conseguimento degli obiettivi per la qualità definiti per i processi e per i prodotti/servizi.

La Direzione verifica la situazione delle competenze professionali per rilevare:

- risultati dell'operatività precedente: Non Conformità, Reclami, mancato raggiungimento degli obiettivi di miglioramento e altre circostanze non positive, le cui cause possono essere rimosse con interventi formativi;
- interventi di formazione ritenuti necessari per consentire agli addetti di ricoprire più efficacemente le mansioni attuali, oppure quelle future;
- necessità di personale formato su particolari temi, argomenti, tecniche, per poter raggiungere i traguardi di miglioramento e di sviluppo commerciale/professionale;
- esigenze di formazione segnalate direttamente dai collaboratori o dai loro Responsabili di Funzione.

Dall'esito della sopra citata verifica deriva il "Piano di Formazione", con cui la Direzione stabilisce le priorità, i periodi di svolgimento, i temi da toccare e le persone interessate.

L'aggiornamento si consegue sostanzialmente con due modalità:

- addestramento sul lavoro: è l'apprendimento delle tecniche operative specifiche, attraverso le quali si perviene alla capacità di svolgere determinate funzioni o mansioni. L'addestramento è svolto prevalentemente sul posto di lavoro;
- formazione generale: è l'apprendimento culturale (manageriale e/o operativo), che permette alla persona di acquisire le conoscenze necessarie per gestire determinate funzioni aziendali e crescere sotto il profilo professionale. Tale formazione, che riguarda anche nuove realtà fino a quel momento non conosciute o trascurate dall'Azienda o dalla persona, può essere svolta sia internamente all'Azienda che presso enti esterni.

Per tutto il personale di nuova assunzione è previsto un ciclo di addestramento sul posto di lavoro, organizzato e coordinato a cura del Responsabile di Funzione al quale sarà assegnato il neo assunto. Tale addestramento comprende sempre anche una sintetica illustrazione delle prescrizioni generali del Sistema Qualità aziendale, con chiarimenti sulla Politica per la Qualità e una formazione più specifica inerente all'area di inserimento. Con le modalità sopra descritte, anche i nuovi assunti sono edotti sulla rilevanza della loro attività nel raggiungimento degli obiettivi per la qualità.

4. IL M.O.G.: CARATTERISTICHE, OBIETTIVI E FINALITÀ

Il M.O.G. previsto dal D.Lgs. 231/01 deve tendere, in prima istanza, a realizzare la cosiddetta condizione "esimente" dalla responsabilità amministrativa della Società, fornendo alla stessa efficaci strumenti per prevenire o contrastare la commissione dei reati richiamati dal Decreto stesso, allo scopo di evitare l'applicazione delle sanzioni amministrative e/o interdittive previste dalla normativa in questione.

Pertanto, in relazione alle aree di attività maggiormente esposte ai rischi di reato sono state elaborate *best practice* e/o protocolli/procedure aziendali allo scopo, non solo di prevenire la commissione dei reati, ma anche di sensibilizzare i soggetti interessati (stakeholders, shareholders, figure apicali a vario titolo, dipendenti, fornitori, etc.) sugli effetti derivanti dalla violazione delle disposizioni previste nel Modello stesso, e renderli consapevoli di poter incorrere in un comportamento potenzialmente illecito, e rilevante penalmente, ed essere passibile di sanzioni disciplinari. Quanto detto, sia nel caso in cui la violazione abbia configurato un reato previsto dal Decreto in esame e quindi abbia provocato una sanzione a carico della Società, sia qualora questa situazione non si sia determinata.

Il Modello prevede la nomina dell'Organismo di Vigilanza, con il compito di vigilare sul funzionamento, sulla efficacia e sulla osservanza del presente documento di Sistema, nonché di curarne l'aggiornamento, come meglio descritto successivamente.

Il Modello si compone di più parti:

MODELLO DI ORGANIZZAZIONE E DI GESTIONE AZIENDALE

- ⇒ L'analisi del rischio di commissione dei reati (risk assessment), dove sono analizzati tutti i reati presupposto e definiti eventuali procedure e/o protocolli atti a limitarne il rischio di commissione (nome file: RA - S.I.O.S.S.);
- ⇒ la presente parte generale, contenente la descrizione del D.Lgs. 231/01 e s.m.i., gli obiettivi dello stesso, i compiti dell'O.d.V. ed il Regolamento Interno dell'Organismo (nome file: MOG – S.I.O.S.S.);
- ⇒ una parte speciale, contenente le procedure ed i protocolli previsti dal risk assessment (nome file: MOG - S.I.O.S.S., è all'interno dello stesso file);
- ⇒ il Codice Etico (nome file: CET - S.I.O.S.S.);
- ⇒ il sistema sanzionatorio all'interno del Sistema Disciplinare (nome file: SD – S.I.O.S.S.).

Il Modello – come da espressa previsione del decreto – è stato implementato sulla base della verifica e della valutazione delle situazioni che comportano rischi di violazione della legge penale, e prevede misure materiali, organizzative e protocolli di comportamento, atti a garantire lo svolgimento dell'attività nel rispetto della legge, con lo scopo ultimo di individuare ed eliminare tempestivamente eventuali situazioni irregolari o di rischio.

Il Modello, in rapporto alla natura, alla dimensione dell'organizzazione e al tipo di attività svolta da **S.I.O.S.S.**, dovrà poter assolvere alle seguenti necessità:

1. individuare le attività nel cui ambito possono essere commessi i reati;
2. prevedere un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo delle situazioni di rischio;
3. prevedere specifici protocolli diretti a programmare la formazione di tutti i soggetti interessati, e l'attuazione delle decisioni dell'azienda in relazione ai reati da prevenire;
4. individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
5. prevedere un'adeguata formazione e informazione del personale sugli aspetti rilevanti ai fini dell'osservanza della legge nello svolgimento dell'attività dell'organizzazione;
6. prevedere un idoneo sistema di controllo sull'attuazione del Modello organizzativo e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate;
7. prevedere il riesame e l'eventuale modifica del Modello organizzativo, quando siano scoperte violazioni significative della legge penale, o in relazione a mutamenti nell'organizzazione o nell'attività, ovvero in relazione all'ampliamento della gamma dei reati prevista dal D.Lgs 231/2001;
8. prevedere obblighi di informazione da parte dell'azienda nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli (O.d.V.);
9. introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

S.I.O.S.S. Infrastrutture S.r.l. ha deciso, dunque, di adottare un M.O.G. (Modello Organizzativo e Gestionale) e di Controllo, conforme alle prescrizioni del D.Lgs 231/2001 e s.m.i., al fine di:

- gestire il rischio di incorrere in sanzioni pecuniarie ed interdittive che possano mettere a rischio l'operatività ordinaria e la continuità aziendale a discapito di tutte le parti interessate;
- consentire all'Organo direttivo (Presidenza e Direzione) di avere un maggior controllo su tutte le aree aziendali e una maggiore garanzia che le attività vengano svolte nel rispetto delle normative vigenti e dei principi etici della società.

5. ATTIVITÀ SVOLTE PER LA PREDISPOSIZIONE DEL MODELLO: LE 5 FASI

La creazione del Modello parte dall'analisi della realtà aziendale e in particolare dall'individuazione delle aree a rischio. Lo scopo è quello di approfondire tutti i processi aziendali evidenziando quelli a rischio, e di proporre specifici protocolli da suggerire al management aziendale per il controllo delle attività e la prevenzione dei rischi.

Si specifica che i protocolli sono diretti all'individuazione di misure peculiari di prevenzione dei reati nelle aree considerate a rischio e comunque nei confronti dell'intera struttura aziendale.

La progettazione e l'implementazione del Modello passa attraverso cinque fasi principali:

1. analisi dei processi, con raccolta dei principali documenti aziendali: struttura dell'Azienda; organigramma con indicazione delle mansioni e dei poteri dei singoli soggetti che lavorano nell'azienda e per l'azienda (Mansionario Organizzativo) – collaboratori esterni; procedure sulla sicurezza del traffico internet, gestione ambientale, etc.;
2. analisi del rischio di commissione dei reati (Risk Assessment);
3. definizione dei protocolli e dei regolamenti interni;
4. nomina dell'Organismo di Vigilanza;
5. attuazione dei Protocolli – comunicazioni all'O.d.V.

Al fine di individuare le aree potenzialmente a rischio all'interno della Sede di Ronchi dei Legionari, è stato necessario attuare una ricognizione delle "fattispecie" penali previste dal Decreto, mettendole in relazione con la situazione aziendale concreta. Tale attività ha dato luogo alla mappatura delle aree a rischio (*Mappatura dei Rischi*) ed all'individuazione delle funzioni-chiave da analizzare (Risk Assessment).

Parallelamente si è provveduto alla redazione del Codice Etico e alla nomina dei componenti l'Organo di Vigilanza previsto dal Modello.

A seguito delle evidenze riscontrate, si è valutato lo "scostamento" tra le misure ritenute necessarie ai fini del Decreto, con il sistema di controllo già in essere. Sono stati individuati i correttivi da apportare alle procedure analizzate, avviando l'adeguamento dei sistemi, in base al concetto di rischio accettabile, attraverso la redazione di procedure e regole che l'azienda dovrà adottare per evitare il compimento dei reati. Uno degli aspetti fondamentali previsti dalla normativa, riguarda la comunicazione e la condivisione del Modello e del Codice Etico. Una volta definito il Modello, sono previste infatti, azioni di comunicazione e formazione rivolte ai soggetti che operano "in" e "per" **S.I.O.S.S.**.

Redatto il Modello, sarà necessario effettuare periodiche verifiche sullo stesso ed eventuali aggiornamenti

(dovuti alla eventuale nascita di nuovi settori aziendali, a modifiche dei ruoli dei vari soggetti che operano “nel” e “per” l’Azienda, a modifiche delle normative di settore, all’eventuale ampliamento della gamma di reati già prevista dal D.Lgs 231/2001, etc.). Tale attività di aggiornamento è di diretta competenza degli organismi societari che dovranno interessare l’Organismo di Vigilanza.

5.1 Fasi dell'intervento

FASE DELL'INTERVENTO	ATTIVITA'
ANALISI	Acquisizione informazioni su processi ed attività
	Analisi dei documenti esistenti
	Mappatura dei Rischi (Risk assessment)
PROGETTAZIONE	Definizione struttura del Modello
	Reati e processi interessati
SVILUPPO	Redazione del Codice Etico
	Nomina Organismo di Vigilanza
	Definizione Protocolli
	Comunicazione e Formazione
GESTIONE	Attuazione dei Protocolli
	Comunicazioni a Organismo di Vigilanza
	Verifiche dell’Organismo di Vigilanza

Alla luce di quanto è emerso dall’analisi complessiva, il Modello contiene le indicazioni necessarie all’azienda per definire gli specifici protocolli e la creazione del relativo sistema sanzionatorio. L’obiettivo, infatti, è quello di rivisitare il sistema di controllo interno, per stabilire procedure *ad hoc* che garantiscano la riduzione ad un livello il minimo possibile il rischio di commissione del reato.

6. DESTINATARI DEL MODELLO

Le regole contenute nel Modello si applicano a coloro che svolgono, in ogni caso e di fatto, funzioni di gestione, amministrazione, direzione o controllo in **S.I.O.S.S.**, ai dipendenti, nonché a coloro i quali, pur non

appartenendo alla Società, operano su mandato della medesima o sono legati alla Società da rapporti di collaborazione, consulenza o altro.

La Società comunica il presente Modello attraverso modalità idonee (Piano di Comunicazione *ad hoc*) ad assicurarne l'effettiva conoscenza da parte di tutti i soggetti interessati. I soggetti ai quali il Modello si rivolge sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società, come anche da Codice civile

S.I.O.S.S. condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello e del Codice Etico, anche qualora il comportamento sia realizzato nell'interesse dell'Azienda, ovvero con l'intenzione di arrecare a essa un vantaggio.

7. ORGANISMO DI VIGILANZA (OdV)

Nel caso in cui si verifichino ipotesi di reati previsti, il Decreto (Art. 6) pone come condizione per la concessione della condizione esimente dalla responsabilità amministrativa, che sia stato affidato a un organismo dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del Modello.

L'azienda ha istituito, con separato atto di nomina, un Organismo con funzioni di vigilanza e controllo (di seguito indicato con la sigla OdV).

I membri dell'OdV, nominati dall'Amministratore Unico, sono più soggetti (Organismo collegiale), secondo le competenze specifiche che si rendono necessarie, e devono assicurare principi di autonomia, indipendenza, professionalità e continuità d'azione necessari per la vigilanza sul sistema.

A tal riguardo, l'azienda mette a disposizione dell'OdV tutte le necessarie risorse idonee a supportarlo nei compiti e nei poteri affidatigli.

7.1 Identificazione, nomina e requisiti dell'Organismo di Vigilanza

In attuazione di quanto previsto dal D.Lgs. 231/01 e s.m.i. viene nominato un Organismo di controllo che possa verificare l'effettiva applicazione delle regole di comportamento e dei Protocolli previsti con il presente Modello. L'incarico di membro dell'Organismo di Vigilanza avrà durata di 3 esercizi, rinnovabili a ciascuna scadenza. La revoca di tale incarico, di competenza dell'Amministratore Unico, sarà ammessa:

- ⇒ per motivi connessi all'inadempimento specifico, sia esso doloso o colposo, agli obblighi di cui all'incarico (ad esempio infedeltà, negligenza, inefficienza, etc.);
- ⇒ nei casi di impossibilità sopravvenuta;
- ⇒ allorquando vengono meno in capo ai membri i requisiti di cui al punto successivo.

Possono essere nominati membri dell'Organismo di Vigilanza, soltanto coloro che presentino i seguenti requisiti di cui alla figura qui a fianco.



In particolare, con riferimento ai reati in violazione delle norme antinfortunistiche e sulla tutela della salute e sicurezza sul lavoro, si precisa che i soggetti candidati a far parte dell'O.d.V. dovranno possedere capacità specifiche in tema di attività ispettiva e consulenziale, dimostrando comprovate competenze nel settore d'attività relativamente agli aspetti di tutela della salute e sicurezza nei luoghi di lavoro, nonché nella conduzione di sistemi di gestione. Ciascun componente è infatti in grado di svolgere le funzioni ed i compiti cui l'OdV è deputato, in relazione all'ambito dei reati per i quali lo stesso è chiamato ad operare.

Per quanto riguarda i candidati esterni all'azienda, questi presenteranno il proprio *curriculum vitae*, che saranno analizzati dalla Direzione aziendale al fine di constatare l'effettiva idoneità. Agli atti verranno conservati la lettera di nomina e i curricula forniti, così come allegati.

7.2 Cause di ineleggibilità dell'Organismo di Vigilanza

Costituiscono motivi di ineleggibilità a componente dell'O.d.V.:

- le circostanze di cui all'articolo 2382 del Codice Civile;
- l'essere indagato per uno o più reati previsti dal D.Lgs. 231/01 e s.m.i.;
- la sentenza di condanna (o di patteggiamento) anche non definitiva, a pena che comporta l'interdizione, anche temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;
- il trovarsi in situazioni che siano in contrapposizione con i principi di autonomia e indipendenza in relazione alle attività da svolgere.

Per le stesse ragioni elencate sopra, i soggetti incaricati a far parte dell'O.d.V. possono altresì essere rimossi dall'incarico (revoca), per cause di sopravvenuta illegittimità a ricoprire la carica.

7.3 Funzioni e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza è affidato il compito di vigilare sui seguenti aspetti:

- effettività dell'applicazione del Modello: ossia vigilare affinché i comportamenti posti in essere all'interno dell'Azienda corrispondano al Modello predisposto;
- efficacia del Modello: ossia verificare che il Modello predisposto sia concretamente idoneo a prevenire il verificarsi dei reati previsti dal Decreto e dalle successive leggi che ne estendano il campo di applicazione;
- collaborazione all'aggiornamento del Modello al fine di adeguarlo ai mutamenti ambientali e alle modifiche della struttura aziendale.

Su un piano più operativo è affidato all'Organismo di Vigilanza il compito di:

- verificare periodicamente la mappa delle aree a rischio reato (o "attività sensibili"), al fine di adeguarle ai mutamenti dell'attività e/o della struttura aziendale. A tal fine, all'Organismo di Vigilanza devono essere segnalate da parte del management e da parte degli addetti alle attività di controllo nell'ambito delle singole funzioni, le eventuali situazioni che possono esporre l'Azienda a rischio di reato. Tutte le comunicazioni devono essere esclusivamente in forma scritta secondo i modelli predisposti;

- effettuare periodicamente, anche attraverso l'eventuale ricorso a professionisti esterni, verifiche volte all'accertamento di quanto previsto dal Modello: in particolare assicurare che le procedure e i controlli previsti siano posti in essere e documentati in maniera conforme e che i principi etici siano rispettati. Si osserva, tuttavia, che le attività di controllo sono demandate alla responsabilità primaria del management operativo e sono considerate parte integrante di ogni processo aziendale (cosiddetto "controllo di linea"), da cui si evince l'importanza di un processo formativo del personale;
- effettuare periodicamente verifiche mirate su operazioni o atti specifici posti in essere soprattutto nell'ambito delle attività sensibili i cui risultati devono essere riassunti in un apposito rapporto che sarà comunicato agli Organi societari;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per uno scambio di informazioni al fine di tenere aggiornate le aree a rischio reato/sensibili con i seguenti obiettivi:
 - ☐ tenere sotto controllo la loro evoluzione al fine di realizzare il costante monitoraggio;
 - ☐ verificare i diversi aspetti attinenti all'attuazione del Modello (definizione di clausole standard, formazione del personale, cambiamenti normativi e organizzativi, ecc.);
 - ☐ garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace siano intraprese tempestivamente;
 - ☐ raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute nel rispetto del Modello. A tal fine, l'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale rilevante e deve essere costantemente informato dal management:
 - a) sugli aspetti dell'attività aziendale che possono esporre l'Azienda al rischio derivante dalla commissione di uno dei reati previsti dal Decreto;
 - b) sui rapporti con Consulenti e Partner;
- verificare che siano attuate le opportune iniziative per la formazione e la comunicazione sul Modello, e far predisporre la documentazione necessaria a tal fine, investendo di ciò il responsabile della formazione;
- interpretare la normativa rilevante e verificare l'adeguatezza del sistema di controllo interno in relazione a tali prescrizioni normative.

La struttura così identificata deve essere in grado di agire nel rispetto dell'esigenza di recepimento, verifica e attuazione dei Modelli richiesti dall'art. 6 del Decreto, ma anche tenendo conto dell'esigenza di costante monitoraggio circa lo stato di attuazione e la effettiva rispondenza degli stessi modelli alle esigenze di prevenzione che la legge richiede. Tale attività di costante verifica deve tendere verso una duplice direzione:

- qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente, è compito dell'Organismo di Vigilanza adottare tutte le iniziative necessarie per far correggere questa "patologica" condizione. Si tratterà, allora, a seconda dei casi e delle circostanze, di far presente alle varie Direzioni le esigenze di:
 - ☐ sollecitare i responsabili delle singole unità organizzative al rispetto del Modello di comportamento;

- ☐ indicare quali correzioni e modificazioni debbano essere apportate alle ordinarie prassi operative;
- ☐ segnalare i casi più gravi di mancata attuazione del Modello;
- qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di adeguamento, sarà proprio l'Organismo stesso a sollecitare gli interventi necessari di adeguamento.

A tal fine, come anticipato, l'Organismo di Vigilanza potrà avere libero accesso alle persone e a tutta la documentazione aziendale, e la possibilità di acquisire dati e informazioni rilevanti dai soggetti responsabili dei processi e degli atti compiuti.

7.4 *Aggiornamento del Modello*

Oltre all'attività di vigilanza che l'Organismo svolge periodicamente sull'attuazione efficace del Modello (e che si estrinseca nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso), l'OdV periodicamente effettua specifiche verifiche sulla reale capacità del Modello di prevenire la commissione dei reati. Tale attività si concretizza in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi dalla Società in relazione alle Attività Sensibili e alla conformità degli stessi ai principi previsti nel Modello e nei relativi Protocolli. Inoltre, viene svolto un esame complessivo di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'Organismo di Vigilanza, degli eventi considerati rischiosi. Le verifiche ed il loro esito dovranno essere illustrate all'Amministratore Unico anche a mezzo di relazioni scritte.

7.5 *Compiti specifici*

L'Organismo di Vigilanza in particolare, dovrà attivarsi per monitorare ed effettuare i debiti controlli in ordine a:

- a) Reati contro la Personalità individuale
- b) Reati in violazione delle norme antinfortunistiche e sulla tutela della salute e sicurezza sul lavoro
- c) Reati contro la Pubblica Amministrazione
- d) Reati Societari
- e) Reati Informatici
- f) Reati di criminalità organizzata transnazionale (art. 3 L. n. 146/2006)
- g) Reati con finalità di terrorismo o di eversione dell'ordine democratico
- h) Reati di ricettazione, riciclaggio, e impiego di denaro beni o utilità di provenienza illecita
- i) Reati contro l'industria e il commercio
- j) Abusi di mercato
- k) Falsità in monete, carte di pubblico credito, valori di bollo e strumenti e segni di riconoscimento
- l) Pratiche di mutilazione degli organi genitali femminili
- m) Reati in materia di violazione dei diritti d'autore
- n) Reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- o) Reati ambientali
- p) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

- q) Reati di corruzione tra privati
- r) Razzismo e xenofobia
- s) Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo
- t) Reati tributari
- u) Contrabbando
- v) Delitti contro il patrimonio culturale;
- w) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici.

7.6 Flussi informativi dall'Organismo di Vigilanza

L'Organismo di Vigilanza riferisce all'Amministratore Unico, in merito all'attuazione del Modello e dei relativi Protocolli, alle attività di verifica e controllo compiute e all'esito delle stesse, segnalando eventuali criticità e proponendo le modifiche al Modello ritenute opportune o necessarie.

Inoltre, l'Odv è stato designato dalla medesima azienda alla gestione del canale di segnalazioni c.d. "Whistleblowing" in accordo al Decreto Legislativo 10 marzo 2023 n. 24 di recepimento della Direttiva (UE) 2019/1937. Esso dovrà redigere la relazione annuale, indirizzata all'Amministratore Unico, relativa alle segnalazioni ricevute ed alle azioni intraprese come meglio definito dalla procedura aziendale attualmente in vigore.

L'Organismo di Vigilanza ha la seguente linea di *reporting*:

- direttamente verso l'Amministratore Unico per la gestione del presente modello:
 - ⇒ proporre all'inizio di ciascun esercizio: il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
 - ⇒ fornire periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, dandone ragione;
 - ⇒ informare immediatamente circa eventuali problematiche significative scaturite dalle attività;
 - ⇒ relazionare, almeno annualmente, in merito all'attuazione del Modello da parte dei Destinatari;

L'istituzione della suddetta linea di *reporting* ha lo scopo di assicurare che l'Organismo di Vigilanza sia in condizione di adempiere alle proprie funzioni con il più alto grado di indipendenza. L'Organismo di Vigilanza potrà, inoltre, comunicare all'Amministratore Unico, valutando le singole circostanze:

- 1) i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturiscano aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'Organismo di Vigilanza ottenga dai responsabili dei processi un piano delle azioni, con relativa tempistica, per le attività suscettibili di miglioramento, nonché le specifiche delle modifiche operative necessarie per realizzare l'implementazione;
- 2) eventuali comportamenti/azioni non in linea con il Codice Etico e con le procedure aziendali, al fine di:
 - acquisire tutti gli elementi per effettuare eventuali comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
 - evitare il ripetersi dell'accadimento, dando indicazioni per la rimozione delle carenze.

Le attività indicate al punto 2), dovranno essere comunicate dall'Organismo di Vigilanza all'Amministratore Unico nel più breve tempo possibile, richiedendo anche il supporto delle altre strutture aziendali, che possono collaborare nell'attività di accertamento e nell'individuazione delle azioni volte a impedire il ripetersi di tali circostanze. Le copie dei relativi verbali saranno custodite dall'Organismo di Vigilanza.

7.7 *Flussi informativi nei confronti dell'Organismo di Vigilanza*

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei dipendenti, responsabili, consulenti, partner, etc., in merito ad eventi che potrebbero ingenerare la responsabilità amministrativa della Società ai sensi del Decreto.

Devono essere obbligatoriamente ed immediatamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- mutamenti nell'organizzazione o nelle attività che possono influire, direttamente o indirettamente, sull'obiettivo di tutela della salute e sicurezza;
- sintesi delle attività di sorveglianza (monitoraggio) e reporting concernenti non conformità gravi, nonché eventuali azioni correttive intraprese;
- accadimento di infortuni e/o segnalazione di malattie professionali che possano avere conseguenze penali;
- eventuali violazioni delle attribuzioni e dei compiti indicati nel Modello, da parte dei soggetti responsabili;
- eventuali provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità (se divulgabili), dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al 589 e 590 del C.p.;
- qualsiasi altra informazione relativa all'attuazione o all'efficacia del Modello;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità (se divulgabili), dai quali si evinca lo svolgimento di indagini per reati;
- le richieste di assistenza legale inoltrate dai dipendenti, dai responsabili in caso di avvio di procedimento giudiziario per reati;
- le notizie relative all'esito di procedimenti disciplinari svolti per mancata osservanza del modello e dei suoi protocolli e alle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative ragioni.

Le informazioni, segnalazioni e *report* previsti nel presente Modello sono conservati dall'Organismo di Vigilanza in un apposito archivio (informatico e/o cartaceo) in modo riservato per un periodo di dieci anni. L'accesso all'archivio è consentito esclusivamente ai membri dell'Organismo di Vigilanza o suoi delegati.

Oltre a quanto sopra esposto, **S.I.O.S.S.** si è dotata di una procedura/policy per la gestione delle eventuali segnalazioni in accordo al Decreto Legislativo 10 marzo 2023 n. 24 di recepimento della Direttiva (UE) 2019/1937, che riguarda *"la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali"*, ha introdotto la nuova disciplina del whistleblowing. Il whistleblowing è uno strumento di derivazione anglosassone attraverso il quale i dipendenti di una organizzazione, pubblica o privata,

segnalano a specifici individui (**S.I.O.S.S.** ha nominato l'Odv quale gestore) una possibile violazione, un reato, un illecito o qualunque condotta irregolare, commessa da altri soggetti appartenenti all'organizzazione. Lo scopo del whistleblowing è quello di permettere alle organizzazioni di affrontare il problema segnalato.

Gli Informatori possono segnalare o divulgare violazioni o tentativi di occultamento di violazioni che si sono verificate o si sospetta si siano verificate in relazione a quanto segue ("Violazioni"):

- A) Reati e illeciti relativi, tra l'altro, ai seguenti comportamenti:
- Corruzione o traffico di influenze;
 - Riciclaggio di denaro, reati finanziari, fiscali e contabili;
 - Conflitti di interesse;
 - Tutela della vita privata e protezione dei dati personali;
 - Pratiche anticoncorrenziali;
 - Sanzioni commerciali, embarghi e controlli sulle esportazioni;
 - Sicurezza e conformità dei prodotti;
 - Salute pubblica;
 - Sicurezza delle reti e dei sistemi informativi;
 - Tutela dell'ambiente;
 - Protezione dei consumatori;
 - Evasione fiscale delle imprese;
 - Frode.
- B) Minaccia o pregiudizio per l'interesse pubblico;
- C) Condotte illecite e rilevanti ai sensi del D.Lgs. 231/2001 o gravi violazioni del Modello Organizzativo 231 e del Codice etico di **S.I.O.S.S.** non coperte dalla direttiva o dalle leggi locali applicabili;
- D) Violazione delle leggi vigenti in materia di molestie morali o sessuali, discriminazione e violenza sul posto di lavoro;
- E) Mancato rispetto dei diritti umani;
- F) Violazione del principio di non ritorsione.

Gli Informatori possono segnalare violazioni che si sono già verificate o quando hanno il ragionevole sospetto che sia altamente probabile che si verifichino violazioni.

Fatti salvi i casi previsti dalla legislazione nazionale vigente, l'Informatore deve essere venuto a conoscenza di tali violazioni nell'ambito della propria attività professionale e, in ogni caso, deve averne avuto conoscenza personale.

È assicurata la massima tutela, riservatezza e protezione all'informatore/segnalante da ritorsioni, illeciti condizionamenti, disagi e discriminazioni di qualunque tipo, per aver debitamente segnalato una violazione in conformità alla Direttiva EU 2019/1937 e al D.Lgs. 24/2023.

8. IL SISTEMA DI DELEGHE E PROCURE

Si intende per delega l'atto interno di attribuzione di funzioni e di compiti, mentre per procura il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti di terzi.

In linea di principio, il sistema di deleghe e procure è caratterizzato da elementi di “sicurezza” ai fini della prevenzione dei reati (rintracciabilità ed evidenziabilità delle operazioni sensibili) e, nel contempo, consentire comunque la gestione efficiente dell’attività aziendale.

Il Sistema delle deleghe e delle procure è inoltre strutturato al fine di stabilire una coerente relazione fra funzione assegnata, responsabilità e poteri.

La Società si impegna a dotarsi, mantenere e comunicare un sistema organizzativo che definisca in modo formalizzato e chiaro l’attribuzione delle responsabilità di gestione, coordinamento e controllo interni, nonché i livelli di dipendenza gerarchica e la descrizione delle mansioni dei dipendenti (per es. organigramma).

Il sistema delle deleghe deve assicurare:

- che l’esercizio del potere sia svolto nell’ambito di posizioni di responsabilità congruenti con l’importanza e/o criticità dell’operazione economica;
- che al processo decisionale prendano parte i soggetti che svolgono le attività oggetto dell’esercizio dei poteri;
- che **S.I.O.S.S.** sia validamente impegnata verso l’esterno da un numero determinato e limitato di soggetti muniti di deleghe o procure formalizzate e opportunamente comunicate (ove si indichino i relativi poteri).

L’OdV effettua verifiche circa la coerenza di eventuali deleghe e/o procure vigenti con la struttura organizzativa di **S.I.O.S.S.**

L’Amministratore Unico ovvero il referente aziendale per la 231, comunica periodicamente all’OdV il sistema di deleghe e procure vigenti e/o relative modifiche. L’OdV opera delle verifiche, con il supporto delle altre funzioni competenti, del sistema di deleghe e procure in vigore e la loro coerenza con l’organigramma in vigore e con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere conferito e/o la qualifica non corrisponda ai poteri di effettiva gestione e rappresentanza, o vi siano altre anomalie.

9. MODALITÀ DI GESTIONE DELLE RISORSE FINANZIARIE

All’interno di **S.I.O.S.S.** l’uso dei contanti è limitato a piccoli acquisti dovuti ad esigenze organizzative puntuali.

Nel Protocollo Amministrazione sono definite le modalità di controllo di attività che investono flussi finanziari.

L’Amministratore Unico ha stabilito dei limiti all’autonomia decisionale della Direzione per l’impiego delle risorse finanziarie.

Esiste sempre una divisione fra chi autorizza la spesa, chi deve dare attuazione all’autorizzazione e chi è deputato alla gestione dei flussi finanziari.

Per le decisioni di impiego delle risorse finanziarie, **S.I.O.S.S.** si avvale di intermediari finanziari e bancari sottoposti ad una regolamentazione di trasparenza e di stabilità conforme a quella adottata negli Stati Membri dell’UE.

Tutte le operazioni che comportano utilizzazione o impegno di risorse economiche o finanziarie devono avere adeguata causale ed essere documentate e registrate, con mezzi manuali o informatici, in conformità a principi di correttezza professionale e contabile; il relativo processo decisionale deve essere verificabile.

Non possono essere corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o altri soggetti, pubblici o privati, in misura non conforme alle prestazioni rese alla Società.

Non possono essere emesse fatture per operazioni inesistenti ovvero occultate o distrutte le scritture contabili al fine di evadere le imposte.

Non possono essere alienate simultaneamente o compiuti altri atti fraudolenti idonei a rendere anche solo parzialmente inefficace la procedura di riscossione coattiva da parte dell'erario.

I finanziamenti a partiti, singoli candidati, associazioni, comitati, organizzazioni e istituzioni devono avvenire nel rispetto della legge e in piena trasparenza.

10. CODICE ETICO

S.I.O.S.S. ha definito apposito Codice Etico che è adeguatamente diffuso internamente, con i dovuti momenti informativi e formativi, e anche verso i soggetti esterni. Il Codice Etico costituisce parte integrante del presente Modello.

11. INFORMAZIONE, FORMAZIONE E COMUNICAZIONE

Ai fini dell'efficacia del presente Modello, è obiettivo della Società di garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei dipendenti. Tale obiettivo riguarda tutte le risorse aziendali che rientrano nelle due categorie anzidette, sia si tratti di risorse già presenti in Società, sia di quelle in via di inserimento.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza in collaborazione con i responsabili delle altre funzioni di volta in volta coinvolte nella applicazione del Modello e sarà articolata sui livelli qui di seguito indicati:

- comunicazione iniziale: L'adozione del presente Modello è comunicata a tutte le risorse presenti in azienda al momento dell'operatività del Modello. Ai dipendenti di nuova assunzione, invece, viene consegnata un'informativa con la quale assicurare agli stessi le conoscenze considerate di primaria rilevanza;
- personale direttivo e con funzioni di rappresentanza dell'Azienda:
 - seminari di aggiornamento nel caso di implementazioni e/o modifiche del Modello;
 - documentazione cartacea e elettronica dedicata all'argomento;
 - e-mail di informazione.
- altro personale:
 - riunione di aggiornamento su eventuali aggiornamenti del Modello e normativa di riferimento;
 - comunicazioni cartacee e/o elettroniche di informazione.

Ad entrambi i livelli di formazione, la partecipazione ai corsi sarà obbligatoria e la frequenza sarà attestata da apposite schede di partecipazione.

Superata la fase iniziale di avvio del sistema, le funzioni aziendali effettueranno ogni utile aggiornamento, modifica e/o integrazione del Modello. Sarà anche compito dell'OdV segnalare l'esigenza di effettuare azioni formative di aggiornamento a fronte di modifiche apportate al Modello o di particolari criticità riscontrate in fase di monitoraggio e controllo dell'applicazione del modello stesso.

Collaboratori Esterni e Partner

L'Organismo di Vigilanza potrà verificare, sempre in funzione dell'operatività del Modello, la congruità di individuazione e scelta da parte della società in ordine a collaborazioni di consulenti, partner o società terze e fornitori in generale.

Informativa a collaboratori esterni e partner

Potranno essere altresì forniti a soggetti esterni alla Società (ad esempio, consulenti e partner) apposite informative sulle politiche e le procedure adottate sulla base del presente Modello organizzativo, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

12. SISTEMA DISCIPLINARE

È stato definito apposito Regolamento Sanzionatorio conforme al CCNL vigente.

Il regolamento sanzionatorio viene reso noto a tutti i dipendenti tramite affissione nei locali aziendali di accesso ai dipendenti stessi. Il regolamento sanzionatorio è parte integrante del Modello.

PARTE SPECIALE

1. PREMESSA

La presente Parte Speciale ha lo scopo di definire le regole di gestione ed i principi di comportamento che tutti i destinatari del Modello dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività svolte in Azienda e considerate "a rischio", la commissione dei reati previsti dal d.lgs. 231/01 e s.m.i. e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

In linea generale, tutti i Destinatari dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi a:

- ✓ Modello di Organizzazione, Gestione e Controllo ai sensi del d.lgs. 231/01 – parte generale e parte speciale;
- ✓ Codice etico;
- ✓ Normativa interna (procedure organizzative).

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

2. PROTOCOLLI DI PREVENZIONE E SISTEMA DEI CONTROLLI

L'art. 6 del Decreto stabilisce, inoltre, che il sistema dei controlli interni deve prevedere, in relazione ai reati da prevenire:

- specifici protocolli per programmare la formazione e l'attuazione delle decisioni dell'Ente;

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

Pertanto, nell'ambito delle attività preordinate alla definizione del Modello, **S.I.O.S.S.** ha provveduto all'identificazione di principi di controllo che devono sovrintendere l'operatività aziendale nell'ambito dei processi gestionali e operativi correlati alle aree a "rischio reato" identificate.

Il sistema dei controlli, realizzato prevede, con riferimento alle attività sensibili individuate:

- **Protocolli di prevenzione generali**, ovvero i principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare gli elementi specifici di controllo;
- **Protocolli di prevenzione specifici** che costituiscono le linee guida di controllo sul processo e che possono trovare maggior declinazione e completamento nell'ambito di altre fonti normative interne della Società (regolamenti, policy, procedure organizzative, istruzioni di lavoro).

3. PROTOCOLLI GENERALI

Il sistema dei controlli, definito da **S.I.O.S.S.** anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, nonché dalle "best practices" nazionali ed internazionali anche in materia di prevenzione della corruzione, è stato costruito applicando i seguenti protocolli generali di prevenzione:

3.1. Norme comportamentali e codici di condotta

Esistenza e diffusione di un Codice Etico aziendale che descriva regole comportamentali di carattere generale a presidio delle attività svolte.

3.2. Poteri autorizzativi e di firma

Esistenza di un sistema di procure e deleghe:

- o coerente con le responsabilità organizzative e di gestione assegnate;
- o contenente la specifica assegnazione di poteri e limiti, anche di approvazione delle spese, dei soggetti titolati;
- o definito nel rispetto dei principi di elaborazione giurisprudenziale e dei requisiti specifici di legge laddove applicabile (ad esempio l'art. 16 del d.lgs. 81/08 e s.m.i. per il caso delle deleghe in materia di sicurezza sul lavoro).

3.3. Procedure e norme interne

Esistenza di regole aziendali, disponibili e conosciute all'interno di **S.I.O.S.S.**, idonee a stabilire responsabilità e modalità operative per lo svolgimento delle attività sensibili e l'archiviazione della documentazione rilevante. La regolamentazione interna declina ruoli e responsabilità di gestione, coordinamento e controllo delle funzioni aziendali a tutti i livelli, descrivendo, in maniera omogenea, le attività proprie di ciascuna struttura.

3.4. Separazione dei compiti

Nell'ambito di ciascun processo aziendale rilevante ai sensi delle Normative di riferimento, al fine di garantire indipendenza ed obiettività, è garantito l'intervento di più soggetti e la separazione delle attività tra coloro che sono incaricati di assumere le decisioni / autorizzare gli atti, eseguire le operazioni stabilite, svolgere sulle stesse gli opportuni controlli previsti dalla legge e dalle procedure del sistema di controllo interno. Un intero processo aziendale, sensibile ai sensi del d.lgs. 231/01 e della L. 190/2012, non può essere affidato ad un unico Soggetto.

3.5. Documentabilità e Tracciabilità

Il processo di decisione, autorizzazione e svolgimento di ciascuna attività sensibile deve essere ricostruibile e verificabile "ex post", attraverso appositi supporti documentali o informatici. In particolare ciascuna operazione/attività relativa ad ogni processo rilevante deve essere adeguatamente documentata; i documenti rilevanti sono opportunamente formalizzati, riportano la data di compilazione e la firma del compilatore/autorizzatore; gli stessi sono archiviati, a cura della funzione competente e con modalità tali da non permettere la modifica successiva se non con apposita evidenza, in luoghi idonei alla conservazione, anche al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare deterioramenti o smarrimenti. Qualora sia previsto l'utilizzo di sistemi informatici per lo svolgimento delle attività sensibili, gli stessi assicurano:

- la corretta imputazione di ogni singola operazione ai soggetti che ne sono responsabili;
- la tracciabilità di ogni operazione effettuata (inserimento, modifica e cancellazione) dai soli utenti abilitati;
- l'archiviazione e conservazione delle registrazioni prodotte.

L'accesso ai documenti archiviati è sempre consentito solo ai soggetti autorizzati (tra cui il Revisore, l'Organismo di Vigilanza ed eventuali altri funzioni di controllo interno opportunamente titolati).

4. PROTOCOLLI SPECIFICI DI PROCESSO

Per i processi / attività "sensibili" / "strumentali" individuati vengono riportati gli elementi di controllo a cui si deve orientare l'operatività degli stessi. Una più dettagliata evidenza di tali protocolli può inoltre essere delegata all'intero corpo normativo aziendale (policy, procedure, istruzioni di lavoro).

4.1. Gestione del fabbisogno e degli acquisti

Responsabile di processo Uffici Acquisti (DTC e CCL/AMG)

Premessa

Il complesso delle procedure e prassi aziendali che già oggi regolano le attività sensibili ed i processi di supporto, dovrà essere applicato nell'ottica della prevenzione dei reati ed alla luce dei "principi di controllo" sotto enunciati. Tali principi di controllo indicano i requisiti del sistema organizzativo – procedurale, necessari per garantire una corretta gestione degli acquisti, nel rispetto degli obiettivi di conformità alle leggi/normative/procedure, e nel contempo di efficacia ed efficienza.

La direzione aziendale dovrà occuparsi di dar disposizioni in modo che, nei rapporti ordinari e straordinari con i fornitori, vengano rispettati i principi e le norme di comportamento sotto elencate oltre a quanto previsto dalla procedura PG-5-0 - Approvvigionamento di prodotti e servizi.

Principi generali

La prevenzione dei reati, tramite l'adozione del Modello organizzativo, deve fondare i suoi presupposti:

- sulla costante verifica circa il rispetto delle procedure interne e dei vari livelli di controllo autorizzativi previsti⁴;
- sull'attività di formazione relativa al Modello di organizzazione, controllo e gestione e alle altre procedure aziendali di **S.I.O.S.S.** nei confronti di tutte le funzioni aziendali, anche tramite programmi di informazione-formazione periodica sui reati commissibili nell'ambito dei rapporti commerciali con i fornitori e relativi sistemi sanzionatori;
- sulla gestione dei rapporti nei confronti dei fornitori, individuando il responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio. In particolare chi intrattiene rapporti con i fornitori per conto di **S.I.O.S.S.**, deve essere conferito uno specifico potere in tal senso dalla stessa Società. Detto potere è specificato nel mansionario e, ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta;
- sulla necessità che i collaboratori esterni siano informati dell'esistenza del presente modello e del Codice etico, inoltre, gli incarichi a loro conferiti, a qualunque titolo questi vengano fatti, devono essere redatti per iscritto, con l'indicazione del compenso pattuito;
- sul prevedere che, con l'esclusione di quelli di modico valore, nessun tipo di pagamento possa esser effettuato in contanti o in natura. Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture ed altri effetti finanziari) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di possibili irregolarità.

È inoltre fatto espresso obbligo ai dipendenti e amministratori di **S.I.O.S.S.**, (di seguito "Destinatari") in via diretta e, tramite apposite clausole contrattuali, anche ai Collaboratori esterni e Partner, di:

⁴ Si osserva che, come conseguenza di ciò, il buon operato dell'OdV dipenderà fondamentalmente dalla verifica del rispetto delle procedure aziendali per ogni processo critico individuato, ripercorrendo a cadenze periodiche, in maniera rotativa e a campione, tutte le fasi critiche in cui si articola l'operato della Società. Tali aspetti valgono "per qualunque fase operativa in cui **S.I.O.S.S.** è attore principale" e dunque verificando l'attività dei soggetti e le autorizzazioni ricevute ai vari livelli operativi.

MODELLO DI ORGANIZZAZIONE E DI GESTIONE AZIENDALE

- ⇒ attenersi alla stretta osservanza di tutte le leggi e regolamenti che disciplinano l'operatività aziendale nelle attività che comportano contatti ordinari e straordinari con i fornitori e con enti e uffici della Pubblica Amministrazione;
- ⇒ gestire qualsiasi rapporto con i fornitori e con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

È fatto invece espresso divieto ai Destinatari in via diretta, e a carico dei Collaboratori esterni e Partner tramite apposite clausole contrattuali, di porre in essere:

- ⇒ comportamenti tali da integrare le fattispecie di reato previste dal Decreto (artt. 24 e 25) e comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato di cui sopra, possano potenzialmente diventarlo;
- ⇒ qualsiasi situazione di conflitto di interessi nei confronti dei fornitori e della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

In particolare, è fatto divieto di:

- ⇒ effettuare prestazioni in favore dei fornitori, outsourcer, consulenti, partner e collaboratori in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- ⇒ effettuare elargizioni in denaro o accordare vantaggi di qualsiasi natura (ad esempio la promessa di assunzione) a fornitori, outsourcer, consulenti, partner, collaboratori in generale e funzionari pubblici;
- ⇒ ricevere o distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta a facilitare o acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo da e per fornitori e funzionari pubblici italiani ed esteri, o loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Come previsto dalle politiche aziendali di **S.I.O.S.S.**, gli omaggi consentiti si dovranno caratterizzare sempre per l'esiguità del loro valore. Tutti i regali offerti o ricevuti - salvo quelli di modico valore - devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo.

Aree sensibili e misure di prevenzione

1. Gestione dei rapporti con i fornitori per gli approvvigionamenti sia nazionali sia internazionali, valutazione dei potenziali fornitori, analisi dell'affidabilità dei fornitori selezionati, definizione dei processi produttivi e degli standard qualitativi, trattative commerciali (prezzo, modalità di fornitura, aspetti tecnico-logistici, tempistiche, etc.);
2. Eventuale assegnazione/gestione di incarichi e di consulenze esterne finalizzate alla gestione dei rapporti con i fornitori (ad esempio, il reperimento di beni, prodotti e servizi, e l'individuazione di mercati su base nazionale e internazionale).

Per le precedenti aree sensibili riportate è necessario:

- ⇒ verificare che alle operazioni aziendali di cui si tratta partecipino i soggetti competenti e a ciò espressamente delegati;
- ⇒ verificare l'esistenza di eventuali conflitti d'interesse con riferimento ai rapporti personali, patrimoniali, giuridici o altro, in essere con i fornitori con cui il personale di **S.I.O.S.S.** intrattenga rapporti con riferimento alle aree sensibili in esame;
- ⇒ effettuare controlli sulla documentazione prodotta anche da enti o tecnici esterni incaricati (certificazioni, analisi, licenze, autorizzazioni in generale, tracciabilità prodotti, etc.);
- ⇒ portare immediatamente a conoscenza dell'Amministratore Unico e all'attenzione all'OdV, eventuali contenziosi/contestazioni e comunque controversie o vertenze;
- ⇒ scegliere gli outsourcer, i consulenti, i partner ed i collaboratori in generale con metodi trasparenti e secondo quanto previsto dai principi espressi nel Codice Etico;
- ⇒ Verificare, tramite gli enti aziendali preposti (ad es. amministrazione, controllo qualità etc.), la corrispondenza tra accordi, ordini di acquisto, contratti, capitolati e specifiche tecniche, etc. Nel caso in cui si verificano gravi discordanze in materia, l'OdV ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta;
- ⇒ verificare il rispetto dei poteri autorizzativi, delle deleghe, delle procure e dei possibili conflitti d'interesse soprattutto nelle persone che conducono incontri e/o intrattengono rapporti con i fornitori;

Elementi di controllo

- **S.I.O.S.S.** assicura che l'acquisizione di lavori, servizi e forniture avvenga nel rispetto dei principi di efficacia, efficienza ed economicità dell'azione amministrativa, oltre che dei principi di libera concorrenza, non discriminazione, proporzionalità, parità di trattamento, sulla base di quanto preliminarmente pianificato dalle funzioni competenti in relazione a criteri verificabili, legati alle esigenze gestionali e di business;
- le Richieste di Acquisto devono contenere le informazioni che consentano di individuare le specifiche tecniche di acquisto e prevedere una nota motivazionale che definisce ragioni e finalità dell'acquisto;
- devono inoltre essere riportate le motivazioni che sottendono l'eventuale indicazione di fornitori specifici a cui richiedere l'offerta;
- Qualora si tratti di interventi in sede (per esempio manutenzioni, installazione macchine, rimozione rifiuti, pulizie ecc.), l'ufficio acquisti richiederà al fornitore anche tutta la documentazione relativa alla sicurezza ed alla regolarità contributiva alla ditta che interverrà;
- In materia di sicurezza sul lavoro, si deve verificare la presenza e congruità dei costi per la sicurezza, l'idoneità tecnico professionale, il contenuto del Piano Operativo di Sicurezza degli appaltatori. Eventualmente consultare il Responsabile del Servizio di Prevenzione e Protezione.

4.1. Protocollo Risorse Umane

Responsabile di processo: AMP – Amministrazione e personale

Premessa

In **S.I.O.S.S.** si sono consolidate nel tempo delle politiche di gestione e sviluppo delle Risorse Umane, improntate ad alcuni principi basilari: correttezza, rispetto, partecipazione, sviluppo delle potenzialità, rigore ed equanimità.

S.I.O.S.S., si è sempre mossa nella direzione di una continua valorizzazione del Fattore Umano, inteso come risorsa essenziale e primaria.

Lo stile di Direzione, pur in qualche misura diversificato nelle varie aree, si è costantemente caratterizzato per una condivisa volontà di coinvolgimento e integrazione sempre più completa di tutti i collaboratori nelle rispettive mansioni, nei ruoli e nelle posizioni organizzative.

Le politiche del personale

Carriera e mobilità del personale

L'azienda gestisce l'evoluzione delle professionalità a disposizione tramite l'identificazione e la valorizzazione delle risorse chiave, degli specialisti e dei "talenti", anche al fine di prevenire cessazioni non auspicabili.

In futuro e qualora necessario, potrebbero essere attivati:

- un monitoraggio di percentuali e ragioni di dimissioni, compresi i neo assunti (interviste);
- pianificazioni dei percorsi di carriera del personale responsabile e con potenzialità;
- coperture delle posizioni vacanti con risorse interne o esterne.

La politica retributiva

Vi è attenzione costante per la politica retributiva, sulla base di tre principi:

- equità esterna: livello medio retributivo rispetto alle aziende del comparto e del territorio;
- equità interna: livello retributivo di collaboratori che svolgono mansioni diverse e di più o meno pari responsabilità all'interno dell'azienda;
- equità individuale: livello retributivo assegnato alla persona in funzione delle sue capacità conoscenze, disponibilità e impegno.

La struttura delle retribuzioni fa riferimento alle seguenti Fonti:

- contratto collettivo nazionale di lavoro;
- integrazioni individuali (RAL);
- incentivi e premi.

Contenzioso e disciplinare

Si tratta di una importante dimensione e strumento gestionale il cui utilizzo deve essere chiaro e condiviso da tutta la struttura.

Rigore e severità vengono coniugati con capacità di comprensione dei fenomeni e dei comportamenti: in ogni caso viene applicato il codice disciplinare derivante dal CCNL vigente. Viene sanzionato con particolare rigore il furto e la appropriazione indebita. Il processo comunicativo e gestionale si svolge come segue:

- a. rilevamento dell'atto a cura del responsabile;

- b. comunicazione ad Amministrazione e Personale (AMP);
- c. redazione lettera di contestazione;
- d. accettazione delle eventuali contro deduzioni (scritte o orali);
- e. irrogazione della sanzione o accoglimento delle controdeduzioni.

Il contenzioso legale viene gestito da Amministrazione e Personale (AMP) con l'eventuale collaborazione di legali esterni specializzati in discipline lavoristiche.

Le strategie

Formazione e addestramento

La procedura da seguire in questo ambito è la "PG-2-0 Competenze, formazione e addestramento delle risorse umane".

Risorse umane e Codice etico

L'adozione da parte dell'azienda del Codice etico e di tutto quanto previsto dal Dlgs 231/2001 e s.m.i. sta coinvolgendo tutti i responsabili e i collaboratori al fine di garantire il rispetto dei principi etici delineati nel Codice, e di preservare l'azienda dal rischio di imputazioni di carattere penale.

Elementi di controllo

S.I.O.S.S. assicura che il processo di ricerca e selezione del personale sia condotto nel rispetto delle Normative vigenti - Nazionali e Comunitarie in materia di reclutamento del personale sulla base dei seguenti principi:

- valorizzazione delle risorse interne e ottimizzazione dell'organizzazione;
- oggettività: la valutazione delle candidature viene effettuata sulla base di requisiti, essenziali e non discriminatori, necessari per la copertura delle posizioni vacanti, definiti precedentemente all'avvio della ricerca;
- imparzialità: per l'individuazione della risorsa si provvede alla predisposizione di una graduatoria dei candidati idonei individuati in funzione della rispondenza ai requisiti predefiniti;
- le candidature sono valutate attraverso un processo di selezione predeterminato e diversamente articolato in funzione delle caratteristiche della posizione e del livello di esperienza richiesto.

L'ufficio preposto, nel rispetto delle Normative Nazionali e Comunitarie applicabili anche nell'ambito delle convenzioni in essere, assicura che il processo di ricerca e selezione del personale avvenga:

- attraverso il confronto di più soggetti candidati idonei rispetto ai requisiti richiesti;
- attraverso il coinvolgimento della funzione richiedente e di **AMP** nella fase di ricerca, valutazione e selezione dei candidati;
- sulla base di una valutazione condivisa delle capacità tecnico-professionali ed attitudinali delle risorse esaminate.

S.I.O.S.S. garantisce:

- che le proposte economico contrattuali siano in linea con le policy interne e/o i CCNL di riferimento ed autorizzate dai Soggetti titolari dell'Azienda;
- che nell'impiego di collaboratori esterni, anche in collaborazione con le funzioni competenti la presenza, nei contratti di collaborazione, vi siano opportune clausole di risoluzione in caso di inosservanza o violazione del Codice Etico e delle previsioni del Modello di Organizzazione,

Gestione e Controllo ai sensi del d.lgs. 231/01 e s.m.i.;

- che i documenti contrattuali relativi all'assunzione e/o collaborazione siano firmati da chi è dotato di procura o delega dalla risorsa interessata;
- e assicura il rispetto degli adempimenti di legge inerenti alle autorizzazioni per le assunzioni agevolate, garantendo, nella predisposizione della relativa documentazione, diligenza e professionalità al fine di fornire agli enti pubblici competenti informazioni chiare, complete e veritiere.

In aggiunta ai protocolli di gestione definiti per il processo di selezione ed assunzione del personale, **S.I.O.S.S.** assicura che il processo di assunzione e/o impiego di cittadini di Paesi Terzi avvenga nel rispetto della Normativa vigente in materia di immigrazione.

4.2. Protocollo Informatico

Responsabile di processo: Amministratore di sistema IT, DIR - Datore di Lavoro

Premessa

Il Sistema Informativo ed Informatico di **S.I.O.S.S.**, che include sistemi di Posta Elettronica, Internet e Intranet (intesa come insieme di applicazioni e di servizi fruibili all'interno della rete aziendale), è di proprietà della società e deve essere utilizzato in accordo con le specifiche direttive impartite. **S.I.O.S.S.** ha affidato ad una società esterna l'amministrazione del sistema informatico.

S.I.O.S.S. si riserva il diritto di monitorare tutti i computer e sistemi elettronici di comunicazione al fine di assicurare, nel legittimo interesse al business della società, il corretto utilizzo dei propri mezzi, come meglio definito nel regolamento informatico.

In particolare, **S.I.O.S.S.** si riserva il diritto di accedere ed utilizzare, in ogni momento e senza darne previa comunicazione, tutte le forme di comunicazione o archiviazione elettronica e computer, inclusi hard driver, dati in utilizzo ai Destinatari per svolgere le proprie funzioni aziendali.

Scopo

Il presente Protocollo è rivolto a tutti gli operatori del sistema informatico di **S.I.O.S.S.** quindi dipendenti, amministratori e consulenti della Società, ove questi ultimi siano autorizzati all'utilizzo del sistema stesso (di seguito "Destinatari").

Lo scopo è quello di indicare in maniera precisa e dettagliata specifiche misure di prevenzione per evitare il concretizzarsi di eventi reato come quelli contemplati nell'art. 24 – bis del D.Lgs. 231/01 - "*Reati Informatici*".

Principi generali

Ai fini dello scopo del presente Protocollo, si è proceduto ad individuare ed eventualmente integrare le procedure in essere (vedi Regolamento per il corretto uso del sistema informativo – cfr. adempimenti GDPR 679/16 Regolamento Europeo Privacy) con l'obiettivo di assicurare innanzitutto il rispetto dei principi generali di cui al Modello 231, nonché i seguenti principi specifici di comportamento:

- ⇒ è vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate;
- ⇒ è vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Conseguentemente, è espresso obbligo dei Destinatari conoscere e rispettare:

- ⇒ Il Regolamento per il corretto uso del sistema informativo con particolare riferimento alle misure di sicurezza atte a garantire l'affidabilità del sistema. Sarà cura dell'azienda, aggiornare tali misure di sicurezza tenendo conto anche dell'evoluzione tecnologica, in particolare per quanto riguarda la sicurezza dei dati trattati, il rischio di distruzione o di perdita ed il rischio di accesso non autorizzato o non consentito;

Uso appropriato dell'accesso ad internet, delle applicazioni e informazioni aziendali

Ogni Responsabile definirà la necessità dell'accesso ad Internet caso per caso, utilizzando come criterio primario quello delle esigenze professionali e conoscitive del singolo operatore di accedere ad Internet per lo svolgimento delle proprie funzioni.

I Destinatari devono essere edotti che l'uso dei computer aziendali e del Network aziendale è soggetto a monitoraggi e la Società effettuerà, a campione, periodici audit sugli accessi ad Internet per verificarne la correttezza ed opportunità. Il controllo avverrà prevalentemente per constatare il rispetto dei seguenti divieti:

- ⇒ visitare siti che contengono materiale pornografico e/o osceno;
- ⇒ inviare e ricevere e-mail particolarmente ampi;
- ⇒ inviare "catene di Sant' Antonio" (chain letters);
- ⇒ condurre attività illegali;
- ⇒ utilizzare un linguaggio improprio indulgendo al turpiloquio e utilizzando termini offensivi sotto il profilo personale nei confronti di qualsiasi interlocutore;
- ⇒ scaricare software commerciali in violazione della legge sul copyright;
- ⇒ scaricare software o file elettronici senza che la presenza di accurate misure di protezione antivirus;
- ⇒ porre in essere qualsiasi tipo di uso inappropriato rispetto alle indicazioni dell'amministratore di sistema.

L'uso delle applicazioni informatiche e delle informazioni aziendali deve essere dedicato esclusivamente alla attività connessa con la mansione e la posizione ricoperta, evitando ogni attività incongrua o non concernente alla propria, e ogni possibile trasmissione di dati e informazioni al di fuori del circuito aziendale. In particolare, ogni utente dovrà anche avere cura di rendere disponibili le informazioni di cui entra in possesso in ragione della propria mansione e posizione, solo e solamente ai propri responsabili, ai colleghi con cui collabora, e, se richiesto, alla Direzione, escludendo l'invio ad altri interlocutori interni che non abbiano titolo o funzione per entrarne in possesso.

La comunicazione del proprio account dovrà tenere conto delle indicazioni di cui sopra, ed essere improntata al principio di cautela e di opportunità.⁵

Conseguenze di un uso inappropriato

Un uso inappropriato o personale della posta elettronica o di Internet da parte dei Destinatari del presente Protocollo, non in accordo quindi con le misure previste in quest'ultimo, comporterà un'azione disciplinare secondo quanto previsto dal Sistema disciplinare contenuto nel Modello.

⁵ In particolare è vietato copiare o esportare informazioni aziendali (documenti, liste, prospetti, mail, etc) dal sistema informativo aziendale utilizzando qualsiasi tipo di supporto (CD, DVD, chiavetta USB, trasferimento elettronico o cartaceo) per scopi non strettamente attinenti allo svolgimento di un particolare compito legato alla propria attività.

Relativamente alle informazioni trasferite, anche solo a voce, a collaboratori e consulenti esterni, esse devono rispondere al requisito di essenzialità. Se si tratta di informazioni riservate o particolari (ex sensibili) devono essere posti in essere gli accorgimenti che ne garantiscano la protezione: mediante la nomina di "addetto al trattamento", come previsto dal Regolamento Europeo sul trattamento dei dati 679/2016 ed eventualmente mediante la sottoscrizione di un "Accordo di Riservatezza e non divulgazione".

Misure di prevenzione

S.I.O.S.S. pur avendo previsto al suo interno il Regolamento per il corretto uso del sistema informativo, da intendersi qui integralmente richiamato, al fine di limitare nella massima misura e pressoché escludere i rischi di responsabilità della Società in relazione ai Reati Informatici di cui all'art. 24-bis del D.Lgs 231 (per cui il presente Protocollo), dovranno inoltre essere rispettate le seguenti misure di prevenzione in relazione alle attività svolte nell'ambito della seguente area sensibile:

- ⇒ effettuazione delle copie di sicurezza delle banche dati trattate, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita (questa indicazione è rivolta in particolare all'Amministratore di Sistema, perché gli utenti in generale non fanno copie di backup);
- ⇒ protezione, mediante l'utilizzo di idonei comportamenti e strumenti elettronici, dei dati sensibili contro l'accesso abusivo da parte di chiunque si introduca nel sistema informatico o telematico attraverso strumenti hardware o software (rootkit, sniffer, keylogger, anonymizer, malicious software);
- ⇒ formazione dei Destinatari al fine di:
 - ☐ renderli edotti dei rischi che incombono sui dati;
 - ☐ renderli edotti delle misure disponibili per prevenire eventi dannosi;
 - ☐ renderli edotti dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
 - ☐ renderli edotti delle responsabilità che ne derivano;
 - ☐ renderli edotti delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
 - ☐ renderli edotti di quanto previsto dal Regolamento Europeo sulla privacy GDPR 679/2016.
- ⇒ segnalazione tempestiva all'Organo di Vigilanza da parte delle funzioni preposte dei casi in cui non venga rispettato il Regolamento per il corretto uso del sistema informativo o siano violate le norme di sicurezza, e nei casi vengano compiute operazioni che possono minare l'effettiva protezione dei dati personali presenti nel sistema o portare all'eventuale intrusione di soggetti non autorizzati nella rete interna (intranet) aziendale.

Elementi di controllo

L'Amministratore di Sistema assicura il processo sistematico di valutazione e gestione del rischio informatico, in particolare con riferimento ai delitti informatici di cui all'art. 24 bis del d.lgs. 231/01 e da quanto previsto dal GDPR 679/2016, attraverso:

- l'identificazione degli obiettivi interni e la definizione dell'ambiente di rischio;
- la valutazione dei rischi connessi alla configurazione di possibili eventi nell'ambito dei processi / attività aziendali;
- l'identificazione delle risposte al rischio in termini di implementazione di opportuni presidi tecnici e di controllo anche di natura organizzativa;
- la definizione delle priorità di intervento e la pianificazione delle attività di controllo, anche in riferimento, in termini di disponibilità dei servizi di business, a quanto emerso da un'opportuna analisi degli impatti

atta a valutare e classificare gli interventi di ripristino alla normale operatività in caso di incidente/disastro;

- il monitoraggio continuo del piano di azione per la gestione dei rischi;
- la corretta gestione delle infrastrutture tecnologiche a supporto delle applicazioni aziendali, nonché dei relativi dispositivi di sicurezza, anche attraverso la definizione e la tenuta sotto controllo di specifici piani di azione per l'acquisizione, il mantenimento, l'aggiornamento e la protezione di dette infrastrutture;
- la disponibilità di ambienti separati per lo sviluppo, il test e la messa in esercizio dei sistemi applicativi di supporto ai processi aziendali;
- la progettazione e l'implementazione, ovvero l'acquisizione, delle applicazioni IT nel rispetto dei requisiti di business tenendo in considerazione i controlli applicativi ed i necessari requisiti di sicurezza - autenticazione, gestione dei log, architettura applicativa;
- l'elaborazione e la diffusione al team di sviluppo di opportune Guidance e Best Practice per la gestione del ciclo di vita del software applicativo;
- la gestione formalizzata e controllata di tutte le modifiche, inclusa la manutenzione di emergenza e le patch, riguardanti sia l'infrastruttura sia le applicazioni in ambiente di produzione, attraverso la registrazione, la valutazione - anche in termini di impatto sui sistemi in esercizio - e l'autorizzazione, da parte dei Soggetti interni titolati, delle modifiche richieste - incluse quelle relative a procedure, processi, parametri di sistema e di servizio;
- il rilascio in produzione dei nuovi sistemi/infrastrutture e delle modifiche a quelli esistenti sulla base di criteri di certificazione concordati e solo a valle di opportune verifiche di quanto implementato ed il confronto con i risultati attesi, attraverso la conduzione di specifici test, anche di integrazione e non regressione, in ambienti dedicati;
- anche per il tramite delle funzioni competenti, l'acquisizione di sistemi e soluzioni da Soggetti terzi previa formalizzazione di opportuni contratti di fornitura integranti clausole di risoluzione e penali in relazione al mancato rispetto di specifici livelli di servizio e requisiti di sicurezza imposti;
- la definizione, l'implementazione, la verifica ed aggiornamento di un piano di continuità dei servizi I.T., anche attraverso la conduzione di un'analisi sugli impatti aziendali e la valutazione dei rischi connessi, che preveda opportune soluzioni di backup, recovery e architetturali ad alta affidabilità;
- la confidenzialità, l'integrità, l'affidabilità e disponibilità dei dati, delle informazioni e delle risorse IT attraverso la formalizzazione, la condivisione con le funzioni interessate e l'attuazione di un Piano di Sicurezza IT contenente le politiche, gli standard e le modalità operative specifiche per la certificazione delle soluzioni informatiche per gli aspetti di sicurezza, per il monitoraggio della stessa, lo svolgimento di test periodici e l'implementazione delle azioni correttive a fronte di punti di debolezza o incidenti identificati;
- l'identificazione univoca di tutti gli utenti ed Incaricati del Trattamento di Dati Personali - interni, esterni o temporanei - e delle loro attività sui sistemi IT - applicazioni aziendali, sistemi operativi, ambienti di sviluppo e manutenzione - l'abilitazione delle relative identità attraverso opportuni meccanismi di autenticazione, l'assegnazione dei diritti di accesso ai sistemi e ai dati in linea con le necessità aziendali e le funzioni ricoperte, nonché nel pieno rispetto del d.lgs. 196/2003 e s.m.i. e del regolamento Europeo 679/2016 in materia di protezione dei dati personali. I diritti di accesso devono essere richiesti dai

responsabili delle funzioni pertinenti, autorizzati dall'Amministratore del Sistema e implementati dalla funzione responsabile della Sicurezza;

- la definizione delle regole per la richiesta, la definizione, il rilascio, la sospensione, la modifica e la revoca, nonché per la revisione ed il monitoraggio, degli identificativi utenti ed i relativi privilegi, per i diversi sistemi e applicazioni aziendali, per tutti gli utenti, inclusi quelli privilegiati quali gli Amministratori di Sistema, sia per i casi normali sia di emergenza;
- l'adozione di un processo di rilevazione e gestione degli incidenti e dei problemi più in generale, che garantisca la loro corretta identificazione, classificazione ed il tempestivo e appropriato trattamento. Tale processo prevede le attività di rilevazione e registrazione degli incidenti e delle richieste di servizio/informazione, la classificazione (severità e impatto), l'adozione di opportune procedure di escalation (funzionali e gerarchiche);
- la sicurezza fisica dei sistemi attraverso l'adozione di opportune modalità operative e procedure di sicurezza adeguate alla protezione da accessi non autorizzati e da danneggiamento, anche accidentale;
- l'adozione di opportune politiche e procedure per la gestione della generazione, modifica, revoca, distruzione, distribuzione, memorizzazione, uso e archiviazione delle chiavi crittografiche;
- l'adozione ed il monitoraggio periodico di opportune procedure anche preventive, sia organizzative sia tecniche, di rilevazione e correzione dei difetti del software ed il controllo puntuale del codice pericoloso (malware) col fine di garantire la protezione dei sistemi informativi e delle tecnologie da possibili rischi di sicurezza;
- l'utilizzo di procedure e tecniche di sicurezza (quali firewalls, dispositivi di sicurezza, segmentazione della rete e rilevazione delle intrusioni) per l'autorizzazione all'accesso ed il controllo del flusso di informazioni da e per la rete aziendale;
- la qualità, tempestività e disponibilità dei dati di business attraverso l'adozione di procedure efficaci per la gestione delle librerie dei supporti di memorizzazione, il salvataggio e il ripristino dei dati, anche attraverso verifiche a campione - da parte di soggetti terzi indipendenti - sulla congruenza dei supporti utilizzati, test di recovery ed inventariazione;
- la formazione e l'addestramento del personale, in fase di assunzione, cambio mansione e utilizzo di nuovi sistemi e applicazioni, al fine di garantire che lo stesso abbia tutte le conoscenze, le competenze e la consapevolezza dei controlli interni e della sicurezza al livello richiesto.

4.3. Protocollo Amministrativo

Responsabile di processo: AMP – Amministrazione e Personale

Premessa

Scopo del presente protocollo è quello di tenere sotto controllo le attività dell'area amministrazione/tesoreria per assicurare che le registrazioni contabili e le rappresentazioni di bilancio siano veritiere e corrette.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli, i soggetti aziendali coinvolti nella gestione delle aree a rischio individuate in relazione ai reati societari di cui all'art. 25 ter del D.Lgs. 231/01 e s.m.i., al fine di prevenire e impedire il verificarsi dei reati, sono tenuti al rispetto di una serie di principi di controllo, basati sull'assunto che la trasparenza e la correttezza contabile si fonda sulla verità, accuratezza e completezza delle informazioni di base per le relative registrazioni contabili. Per ogni operazione contabile deve essere conservata agli atti sociali una adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

- a) l'agevole registrazione contabile;
- b) l'individuazione dei diversi livelli di responsabilità;
- c) la ricostruzione accurata delle operazioni, anche al fine di ridurre la probabilità di errori interpretativi.

Il sistema di controllo di **S.I.O.S.S.** è costituito nelle sue linee generali secondo i principi di controllo, descritti ai punti seguenti.

Tracciabilità delle operazioni/atti

Ogni operazione o fatto gestionale sensibile e/o rilevante è documentato, coerente e congruo, così che in ogni momento è possibile identificare la responsabilità di chi ha operato (valutato, deciso, autorizzato, effettuato, controllato l'operazione).

Segregazione delle funzioni

All'interno di un processo aziendale, funzioni separate decidono un'operazione, l'autorizzano, eseguono operativamente, registrano e controllano. Una contrapposizione tra responsabilità risulta teoricamente opportuna in quanto disincentiva la commissione di errori od irregolarità da parte di una funzione ed eventualmente ne permette l'individuazione da un'altra coinvolta nel processo.

Evidenza formale dei controlli

I controlli effettuati all'interno di un processo o una procedura sono adeguatamente formalizzati e documentati, così che si possa, anche in un momento successivo, identificare chi ha eseguito un controllo ed il suo operato.

La responsabilità di una operazione/processo aziendale è chiaramente e completamente conosciuta all'interno dell'organizzazione.

Formalizzazione ed archiviazione documenti rilevanti

Alla luce dei principi generali di controllo appena evidenziati, è necessario che tutte le operazioni svolte nell'ambito delle attività "sensibili" ricevano debita evidenza.

Nell'esecuzione di tali operazioni, occorre che sia garantito il rispetto dei principi di comportamento di seguito indicati:

- ⇒ astenersi dal porre in essere condotte tali da integrare le fattispecie di reati societari contenute nel documento di sistema;
- ⇒ garantire il rispetto delle regole comportamentali previste nel Codice Etico di **S.I.O.S.S.**, con particolare riguardo all'esigenza di assicurare che ogni operazione e transazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua;
- ⇒ tenere nella formazione del bilancio un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni necessarie per consentire di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società, anche al fine di fornire ai soci e ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società, sull'evoluzione della sua attività;
- ⇒ osservare le prescrizioni imposte dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo;
- ⇒ astenersi dal compiere qualsivoglia operazione o iniziativa qualora vi sia una situazione di conflitto di interessi, ovvero qualora sussista, anche per conto di terzi, un interesse in conflitto con quello della Società;
- ⇒ assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale prevista dalla legge, nonché la libera formazione della volontà assembleare;
- ⇒ astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false, non corrette o fuorvianti, idonee a provocare l'alterazione del prezzo di strumenti finanziari;
- ⇒ gestire con la massima correttezza e trasparenza il rapporto con le Pubbliche Autorità;
- ⇒ non emettere fatture per operazioni inesistenti;
- ⇒ non occultare o distruggere le scritture contabili al fine di evadere le imposte;
- ⇒ non alienare simulatamente o compiere altri atti fraudolenti idonei a rendere anche solo parzialmente inefficace la procedura di riscossione coattiva da parte dell'erario.

L'OdV sarà informato su qualsiasi operazione realizzata dai soggetti sopra indicati solo e solamente nel caso in cui sia valutata potenzialmente a rischio di commissione di reato, circa il quale dovrà essere fornita evidenza scritta.

In ogni caso, si dovrà tener conto, per quanto riguarda le specifiche fattispecie di reato di seguito indicate, delle seguenti previsioni.

Le comunicazioni sociali

Per la prevenzione dei reati relativi alla predisposizione delle comunicazioni indirizzate ai soci e ai terzi interessati, nonché ai fini della formazione del bilancio è necessario che la procedura seguita in azienda garantisca:

- ⇒ il rispetto dei principi di compilazione dei documenti contabili di cui al C.c.;
- ⇒ il rispetto del principio di completezza del bilancio, mediante l'indicazione di tutti i dati prescritti dalla normativa vigente (C.c.), e la sua trasmissione alla Direzione **DIR** e agli Organi di controllo;
- ⇒ la tracciabilità delle operazioni che comportino il trasferimento e/o il differimento di posizioni creditorie al fine di evitare situazioni a rischio.

Conflitti di interesse

In materia di conflitti di interesse, è necessario che la procedura seguita in azienda garantisca la definizione dei casi in cui si potrebbero verificare i conflitti di interesse, prevedendo:

- ⇒ la raccolta di una dichiarazione di assenza di conflitti di interesse e del rispetto del Codice Etico dal management della Società.

Gestione contante e carte di credito

In **S.I.O.S.S.** l'uso dei contanti è limitato a piccoli acquisti/ vendite preventivamente autorizzati. Tutte le altre operazioni finanziarie avvengono e devono avvenire mediante l'utilizzo di conti correnti bancari e solo dopo l'autorizzazione dei responsabili muniti di adeguati poteri.

In azienda vengono utilizzate carte di credito con limite di spesa stabilito in funzione della posizione e del ruolo ricoperti dall'assegnatario. Il superiore gerarchico dell'assegnatario della carta di credito approva ed autorizza la spesa se ritenuta congrua.

Gestione finanziaria

La procedura che regola la gestione finanziaria (pagamenti), ai fini della prevenzione dei reati societari, per la corretta imputazione dei costi e per il controllo incrociato, è la seguente:

- Arrivo materiali in sede;
- Verifica da parte di AMG (Gestione Magazzino) della congruenza tra Documento di Trasporto (DDT) e materiali consegnati;
- Ricezione fattura da parte di AMP (Amministrazione e Personale) sul sistema di interscambio;
- Controllo congruenza tra Fattura e DDT (controllo quantitativo);
- Registrazione fatture: sono salvate nel server aziendale, una copia di cortesia ad uso amministrativo sarà oggetto dei successivi controlli ed approvazioni da parte delle diverse figure aziendali:
 - Apposizione timbro con: data, n. protocollo, codice, importo – Amministrazione
 - Visto registrazione (responsabile Amministrazione)
 - Visto pagamento (ufficio acquisti – in questo momento viene effettuato il confronto con l'ordine o il contratto in essere con il fornitore);
 - Controllo Prezzo
 - Autorizzazione al pagamento da parte della direzione
- Ordine di pagamento.

4.4. Protocollo pubblica amministrazione

Responsabile di processo: AMP - Amministrazione e Personale, DIR - Direzione Generale

Premessa

L'insieme delle procedure e delle prassi aziendali che già oggi regolano le attività sensibili ed i processi di supporto, dovrà essere applicato nell'ottica della prevenzione dei reati ed alla luce dei "principi di controllo" sotto enunciati. Tali principi di controllo indicano i requisiti del sistema organizzativo – procedurale, necessari per garantire una corretta gestione, nel rispetto degli obiettivi di conformità alle leggi/normative/procedure, oltre che di efficacia ed efficienza.

La direzione dovrà occuparsi di dar disposizioni in modo che si abbiano rapporti con la Pubblica Amministrazione, vengano rispettati i principi e le norme di comportamento sotto elencate.

Principi generali

La prevenzione dei reati, tramite l'adozione del Modello Organizzativo, deve fondare i suoi presupposti:

- sulla costante verifica circa il rispetto delle procedure interne e dei vari livelli di controllo autorizzativi previsti⁶;
- sull'attività di formazione relativa al Modello di organizzazione, controllo e gestione e alle altre procedure aziendali di **S.I.O.S.S.** nei confronti di tutte le funzioni aziendali, anche tramite programmi di informazione-formazione periodica di amministratori, di soggetti apicali e dipendenti in generale, sui reati contro la Pubblica Amministrazione e i relativi sistemi sanzionatori;
- sulla gestione dei rapporti nei confronti della P.A. in modo unitario, individuando il responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio. In particolare a chi intrattiene rapporti con la P.A. per conto di **S.I.O.S.S.** deve essere conferito un potere in tal senso dalla stessa Società. Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta;
- sul fatto che i collaboratori esterni siano informati dell'esistenza del presente modello e del codice etico; inoltre, gli incarichi a loro conferiti, a qualunque titolo questi vengano fatti, devono essere redatti per iscritto, con l'indicazione del compenso pattuito;
- sulla previsione che, con l'esclusione di quelli di modico valore, nessun tipo di pagamento possa esser effettuato in contanti o in natura. Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari), devono porre particolare attenzione all'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di possibili irregolarità.

È inoltre fatto espresso **obbligo** ai dipendenti, apicali e amministratori di **S.I.O.S.S.** (di seguito "Destinatari") in via diretta e, tramite apposite clausole contrattuali, anche ai collaboratori esterni e partner, di:

⁶ Si osserva che, come conseguenza di ciò, il buon operato dell'O.d.V. dipenderà fondamentalmente dalla verifica del rispetto delle procedure aziendali per ogni processo critico individuato, ripercorrendo a cadenze periodiche, a rotazione e a campione, tutte le fasi critiche in cui si articola l'operato della Società. Tali aspetti valgono "per qualunque fase operativa in cui **S.I.O.S.S.** è attore principale", e dunque verificando l'attività dei soggetti e le autorizzazioni ricevute ai vari livelli operativi.

MODELLO DI ORGANIZZAZIONE E DI GESTIONE AZIENDALE

- ⇒ attenersi alla stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, anche nelle attività che comportano contatti e rapporti con la Pubblica Amministrazione e nelle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
- ⇒ gestire qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

È fatto invece espresso **divieto** ai Destinatari in via diretta, e a carico dei collaboratori esterni e partner, tramite apposite clausole contrattuali, di porre in essere:

- ⇒ comportamenti tali da integrare le fattispecie di reato previste dal Decreto (artt. 24 e 25 del Decreto) e comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato di cui sopra, possano potenzialmente diventarlo;
- ⇒ qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato;
- ⇒ effettuare prestazioni in favore di outsourcer, consulenti, partner e collaboratori in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- ⇒ effettuare elargizioni in denaro o accordare vantaggi di qualsiasi natura (ad esempio la promessa di assunzione) a funzionari pubblici o persone con questi collegate;
- ⇒ distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio, o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Come previsto dalla politica aziendale di **S.I.O.S.S.**, gli omaggi consentiti si dovranno caratterizzare sempre per l'esiguità del loro valore. Tutti i regali offerti - salvo quelli di modico valore - devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo.

Aree sensibili e misure di prevenzione

Rapporti con la Pubblica Amministrazione:

- A. Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni, licenze, concessioni per l'esercizio delle attività aziendali;
- B. Assegnazione/gestione degli incarichi e delle consulenze esterne finalizzate alla gestione dei rapporti con soggetti pubblici (con particolare riferimento al controllo della sicurezza dei luoghi di lavoro).

Per le precedenti aree sensibili riportate è necessario:

- ⇒ verificare che, durante eventuali ispezioni giudiziarie, tributarie e amministrative e quelle poste in essere dalle Autorità di Vigilanza di settore (quali ad esempio quelle preposte alla verifica del rispetto del D.Lgs. 81/08, del D.Lgs 106/09 e s.m.i., alle verifiche tributarie, dell'INPS e dell'INAIL, ai rapporti con le Aziende Sanitarie e con i Comuni) nonché in ogni atto propedeutico alla richiesta di autorizzazioni, licenze o altro, partecipino i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono

essere redatti e conservati gli appositi verbali. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta;

- ⇒ verificare l'esistenza di eventuali conflitti d'interesse con riferimento ai rapporti personali, patrimoniali, giuridici o altro in essere con i soggetti fisici/giuridici della Pubblica Amministrazione con cui il personale di **S.I.O.S.S.** dovesse intrattenere rapporti, con riferimento alle aree sensibili in esame (ovvero, sia durante le ispezioni/controlli, sia durante la richiesta di autorizzazioni, licenze, concessioni o altro);
- ⇒ effettuare controlli sulla documentazione prodotta anche da tecnici esterni incaricati, per la richiesta di ogni tipo di autorizzazione, licenza, concessione o altro - per esempio a titolo meramente esemplificativo ma non esaustivo:
 - richiesta di omologazione e revisione impianti e sistemi di sicurezza;
 - documentazione relativa allo smaltimento dei rifiuti nel rispetto delle autorizzazioni richieste e da richiedere, o rinnovare, o comunicare alle autorità competenti anche a mezzo della gestione corretta dei documenti (registri di carico e scarico dei rifiuti) e a mezzo di ditte convenzionate terze;
 - documentazione relativa all'ottenimento dei certificati di prevenzione incendi e/o al soddisfacimento delle richieste da parte degli organi preposti alla vigilanza sui rischi ed incendi;
 - documentazione connessa alla sicurezza dei luoghi di lavoro ivi comprese le norme sulla osservanza delle leggi sanitarie;
- ⇒ assicurare la tracciabilità e verificabilità ex post delle transazioni fatte con la Pubblica Amministrazione tramite adeguati supporti documentali/informativi;
- ⇒ portare immediatamente a conoscenza della direzione aziendale e all'attenzione all'OdV, eventuali contenziosi/contestazioni e, più genericamente, ogni problema con la Pubblica Amministrazione;
- ⇒ scegliere gli outsourcer, i consulenti, i partner ed i collaboratori in generale con metodi trasparenti e secondo l'esistente procedura aziendale.

Rapporti indiretti con la Pubblica Amministrazione

1) Gestione della liquidità e contabilità

Con riferimento a tale area sensibile l'Organismo di Vigilanza dovrà:

- ⇒ verificare a campione la corrispondenza tra accordi, ordini di acquisto, vendite, fatturazioni, incassi, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; effettuare controlli sui report gestionali, flussi finanziari e riconciliazioni bancarie⁷; effettuare controlli sulla documentazione societaria e sulla fatturazione passiva.

2) Gestione dei rapporti con l'amministrazione finanziaria

Con riferimento a tale area sensibile è necessario:

- ⇒ fare in modo che, alle eventuali ispezioni giudiziarie, tributarie e amministrative o a quelle poste in essere dalle Autorità di Vigilanza di settore (quali ad esempio quelle preposte al rispetto del D.lgs. 81/08,

⁷ In particolare, per quanto attiene al ciclo incassi e pagamenti, rientrante infra flussi finanziari e riconciliazioni bancarie, ogni attività (come precisato dalle linee guida), deve essere registrata, documentata e verificabile con immediatezza. Per nessuna ragione, è consentito che le risorse finanziarie dell'ente e la relativa movimentazione possano non essere registrati documentalmente; considerata la scarsa presenza di denaro contante, esso dovrà essere conservato in una cassetta con chiave della cui custodia dovranno essere preventivamente individuati i responsabili. È vietato in particolare fatturare prestazioni non erogate, duplicare la fatturazione, non emettere note di credito qualora siano state fatturate, per errore, prestazioni in tutto o in parte inesistenti.

del D.lgs 106/09 e s.m.i., alle verifiche tributarie, dell'INPS e dell'INAIL), partecipino i soggetti a ciò espressamente delegati.

Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta.

3) Gestione affari legali ed attività giudiziale e stragiudiziale

Con riferimento a tale area sensibile è necessario:

- ⇒ verificare il rispetto dei poteri autorizzativi, delle deleghe, delle procure, dei possibili conflitti d'interesse soprattutto nelle persone che conducono incontri e/o intrattengono rapporti con la Pubblica Amministrazione;

4) Gestione dell'omaggistica e delle donazioni nei confronti dei soggetti pubblici

Con riferimento a tale area sensibile è necessario:

- ⇒ procedere alla verifica dell'effettiva conoscenza del Modello e dei programmi di formazione-informazione sulle disposizioni di cui al Decreto in capo a tutti i Collaboratori in generale della Società;
- ⇒ vietare elargizioni in denaro o accordare vantaggi di qualsiasi natura (ad esempio la promessa di assunzione) a funzionari pubblici incaricati anche dei controlli nell'ambito delle norme antinfortunistiche e della tutela dell'igiene e della salute sul lavoro;
- ⇒ vietare la distribuzione di omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;
- ⇒ verificare il rispetto dei principi e delle procedure già previste all'interno del Codice Etico.

Rapporti diretti con la Pubblica Amministrazione

Gestione dei contributi pubblici (Regione, Provincia etc.).

Con riferimento a tale area sensibile è necessario seguire le seguenti procedure:

- ⇒ le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi o finanziamenti, devono contenere solo elementi veritieri e l'impegno della società beneficiaria, in caso di ottenimento degli stessi, all'effettiva utilizzazione dei fondi ottenuti, secondo le finalità previste dalla specifica normativa di riferimento;
- ⇒ coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, etc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente al Comitato di Vigilanza eventuali situazioni di irregolarità o anomalie.

4.5. Protocollo anticorruzione

Premessa

Il complesso delle procedure e prassi aziendali che già oggi regolano le attività sensibili ed i processi di supporto, dovrà essere applicato nell'ottica della prevenzione dei reati ed alla luce dei "principi di controllo" sotto enunciati. Tali principi di controllo indicano i requisiti del sistema organizzativo – procedurale, necessari per garantire dei comportamenti atti ad evitare ogni ipotesi di corruzione e/o induzione indebita a dare o promettere utilità nei rapporti tra privati (stakeholders e shareholders), e con la pubblica amministrazione, nel rispetto degli obiettivi di conformità alle leggi/normative/procedure.

I responsabili delle varie funzioni aziendali dovranno dare disposizioni in modo che, nei rapporti ordinari e straordinari con tutti gli interlocutori aziendali, vengano rispettati i principi e le norme di comportamento sotto elencate.

Principi generali

La prevenzione dei reati, tramite l'adozione del Modello Organizzativo, deve fondare i suoi presupposti:

- sulla costante verifica circa il rispetto delle procedure interne e dei vari livelli di controllo autorizzativi previsti⁸;
- sull'attività di formazione relativa al Modello di organizzazione, controllo e gestione e alle altre procedure aziendali di **S.I.O.S.S.**, nei confronti di tutte le funzioni aziendali, anche tramite programmi di informazione-formazione periodica di amministratori, di soggetti apicali e dipendenti in genere sui reati commissibili in tema di corruzione tra privati e induzione indebita a dare o promettere utilità, nell'ambito dei rapporti con tutta la platea degli interlocutori aziendali e relativi sistemi sanzionatori;
- sulla gestione dei rapporti nei confronti dei fornitori, individuando il responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio. In particolare ai Dipendenti, Amministratori, che intrattengono rapporti con i fornitori per conto della Società deve essere conferito uno specifico potere in tal senso dalla stessa Società. Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta;
- sulla necessità che i collaboratori esterni siano informati dell'esistenza del presente modello e del Codice etico, e inoltre, gli incarichi a loro conferiti, a qualunque titolo questi vengano fatti, devono essere redatti per iscritto, con l'indicazione del compenso pattuito;
- sul prevedere che, con l'esclusione di quelli di modico valore, nessun tipo di pagamento possa esser effettuato in contanti o in natura. Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture ed altri effetti finanziari) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di possibili irregolarità.

È inoltre fatto espresso obbligo ai dipendenti, dirigenti e amministratori di **S.I.O.S.S.**, (di seguito "Destinatari") in via diretta e, tramite apposite clausole contrattuali, anche ai Collaboratori esterni e Partner, di:

⁸ Si osserva che, come conseguenza di ciò, il buon operato dell'OdV dipenderà fondamentalmente dalla verifica del rispetto delle procedure aziendali per ogni processo critico individuato, ripercorrendo a cadenze periodiche, in maniera rotativa e a campione, tutte le fasi critiche in cui si articola l'operato della Società. Tali aspetti valgono "per qualunque fase operativa in cui **S.I.O.S.S.** è attore principale" e dunque verificando l'attività dei soggetti e le autorizzazioni ricevute ai vari livelli operativi.

- ⇒ attenersi alla stretta osservanza di tutte le leggi e regolamenti che disciplinano l'operatività aziendale nelle attività che comportano contatti ordinari e straordinari con i fornitori e con enti e uffici della Pubblica Amministrazione;
- ⇒ gestire qualsiasi rapporto con i fornitori, i clienti e con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

È fatto invece espresso divieto ai Destinatari in via diretta, e a carico dei Collaboratori esterni e Partner, di porre in essere *comportamenti tali da integrare le fattispecie di reato previste dalla Legge "Anticorruzione" n.190 del 6.11.2012 – Nuovi reati presupposto della Responsabilità Amministrativa D.Lgs. 231/01: "Corruzione tra privati" e "Induzione indebita a dare o promettere utilità"*.

Qualsiasi situazione di conflitto di interessi nei confronti dei fornitori, dei clienti e della Pubblica Amministrazione in relazione a quanto previsto dalle sopradette ipotesi di reato.

In particolare, è fatto divieto di:

- effettuare prestazioni in favore dei fornitori, outsourcer, consulenti, partner e collaboratori in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- effettuare elargizioni in denaro o accordare vantaggi di qualsiasi natura (ad esempio la promessa di assunzione) a fornitori, outsourcer, consulenti, partner, collaboratori in generale e funzionari pubblici;
- ricevere o distribuire utilità, omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta a facilitare o acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo da e per fornitori e funzionari pubblici italiani ed esteri, o loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda o per l'interlocutore. Come previsto dalle politiche aziendali di **S.I.O.S.S.**, gli omaggi consentiti si dovranno caratterizzare sempre per l'esiguità del loro valore. Tutte le utilità o i regali offerti o ricevuti - salvo quelli di modico valore - devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo.

La legislazione di riferimento, le aree sensibili e le misure di prevenzione

Con la Legge n. 190 del 6.11.2012, pubblicata nella Gazzetta Ufficiale del 13.11.2012, il Legislatore italiano ha inteso adeguare la normativa nazionale ai dettami della Convenzione di Strasburgo del 27 gennaio 1999, ratificata con Legge n. 110 del 28.6.2012.

La L. 190/12 è intitolata: "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"; interviene su un duplice fronte:

- 1) detta disposizioni per la prevenzione, individuando e regolamentando una "Autorità nazionale anticorruzione", imponendo nuovi obblighi alle Pubbliche Amministrazioni, a valere anche per le società partecipate dalle stesse e per le loro controllate (limitatamente alle attività di pubblico interesse), apportando modifiche normative e delegando al Governo ulteriori interventi in materia (L. 190/12 art. 1 co. da 1 a 74);

2) interviene sul fronte della repressione, innovando la disciplina del codice penale quanto ai reati di concussione e corruzione, modificando l'art. 2635 c.c. in tema di corruzione tra privati ed introducendo nuovi reati presupposto della Responsabilità Amministrativa D.Lgs. 231/01 (L. 190/12 art. 1 co. 75 e ss.).

La corruzione tra privati

L'art. 1 co. 76 L. 190/2012 modifica l'art. 2635 c.c. e introduce il reato di "corruzione tra privati".

Premesso che il legislatore si è discostato dal dettato della Convenzione di Strasburgo, rimanendo legato nella sostanza al precedente reato di "Infedeltà a seguito di dazione o promessa di utilità" di cui al vecchio art. 2635 c.c., la normativa italiana, nella L. 190/2012 ha invece disposto che **il reato si perfeziona solo quando il soggetto compie od omette in concreto atti in violazione dei propri obblighi e alla società derivi di fatto un nocumento**.

Per la normativa italiana non si tratta dunque di vera corruzione tra soggetti privati, ma di un "reato societario", essendo solo una violazione nei rapporti tra soggetto ed ente per cui opera.

Il reato sussiste dunque solo se chi riceve il vantaggio indebito viene meno ai propri obblighi verso la propria società e se causa un nocumento alla società stessa, altrimenti l'atto corruttivo non è perseguito.

Il reato così come previsto dal legislatore italiano non è perciò diretto a garantire un comportamento etico sul mercato e nella concorrenza.

Estensione dei reati presupposto causa di Responsabilità Amministrativa D.Lgs. 231/01

L'art. 1 co. 77 L. 190/2012 introduce tra i reati presupposto della Responsabilità Amministrativa D.Lgs. 231/01:

- all'art. 25 D.Lgs. 231/01 il reato di "Induzione indebita a dare o promettere utilità" (art. 319-quater c.p.),
- alla nuova lettera s-bis dell'art. 25-ter il reato di "Corruzione tra privati", quanto alla sola condotta attiva del corruttore (art. 2635 co. 3 c.c.).

L'introduzione nel D.Lgs. 231/01 dell'art. 319 quater c.p., in realtà, nulla innova, in quanto la condotta ora prevista come reato presupposto era già contemplata dal vecchio art. 317 c.p. che già costituiva reato presupposto.

È invece confermata la "Corruzione tra privati" dal lato attivo del corruttore, così come prevista dall'art. 2635 co. 3 c.c.

4.6. Gestione degli aspetti ambientali

Responsabile di processo: GSA – Responsabile Gestione Ambientale

Premessa

Scopo del presente protocollo è quello monitorare le attività e le autorizzazioni ambientali di **S.I.O.S.S.** in accordo alle procedure ed istruzioni operative in essere.

- PG-10-0 Identificazione degli aspetti ambientali e valutazione della significatività
- PO-12-0 Controllo operativo e monitoraggio del sistema di gestione ambientale
- PO-13-0 Sorveglianza e misurazioni ambientali
- PO-14-0 Manipolazione, stoccaggio e smaltimento rifiuti
- IO-16-0 Gestione dei rifiuti da demolizione e dei materiali di scavo

S.I.O.S.S. ha la certificazione ISO 14001, perciò tutta la gestione ambientale avviene mediante procedure ed istruzioni operative validate da ente terzo.

Nell'ambito dei reati ambientali, previsti dal decreto 231/01 e s.m.i., sono valutate a “rischio” le attività sociali relative a:

- a) gestione dei rifiuti, con particolare riferimento alla discarica per rifiuti non pericolosi e degli annessi impianti di selezione e inertizzazione;
- b) scarico acque reflue;
- c) inquinamento di suolo, sottosuolo, acque;
- d) emissioni in atmosfera;
- e) sostanze lesive dell'ozono;
- f) coltivazione di cave;
- g) trasporto di merci varie, compresi i rifiuti prodotti anche da terzi;
- h) logistica portuale, comprese le attività di imbarco e sbarco merci anche alla rinfusa e deposito di prodotti energetici;
- i) inquinamento doloso e colposo provocato dalle navi alla qualità delle acque;
- j) distruzione di specie animali o vegetali protette;
- k) deterioramento di habitat protetti.

Nello specifico S.I.O.S.S. potrebbe incorrere nei reati di cui alle lettere a), b), c), d), g).

Con riferimento alla politica ambientale, siano definiti:

- ⇒ un sistema formalizzato volto a gestire le tematiche ambientali, negli obiettivi generali che la stessa si è proposta di raggiungere;
- ⇒ l'impegno a garantire la conformità con le leggi applicabili in materia;
- ⇒ la presenza di un processo di comunicazione interna ed esterna;
- ⇒ un processo strutturato di aggiornamento periodico.

Con riferimento ai soggetti responsabili di attività aventi potenziali impatti sull'ambiente, siano definiti:

- ⇒ un sistema di formale attribuzione delle responsabilità tramite deleghe e procure formalmente accettate;
- ⇒ un organigramma che includa le funzioni aziendali la cui attività ha potenziali impatti sull'ambiente;
- ⇒ i requisiti minimi specifici – da verificare periodicamente – delle singole funzioni, coerentemente alle esigenze organizzative ed alle disposizioni di legge in materia (ad es. pregressa esperienza, titoli specifici, competenze e formazione, ecc.);
- ⇒ un documento che descriva le funzioni pertinenti alle attività dell'organizzazione;
- ⇒ l'individuazione di soggetti che svolgono attività potenzialmente impattanti sull'ambiente, definendo i loro compiti e le connesse responsabilità;
- ⇒ la definizione delle competenze che i soggetti con responsabilità in ambito ambientale devono possedere.

Con riferimento al controllo della legislazione, siano definiti:

- ⇒ i ruoli e le responsabilità con riferimento alle informazioni inerenti agli aspetti normativi rilevanti e le prescrizioni applicabili in materia ambientale;
- ⇒ i criteri e le modalità per l'aggiornamento normativo e per la relativa comunicazione alle aree aziendali interessate;
- ⇒ i criteri e le modalità per la verifica dell'evoluzione della best practice e delle norme tecniche in materia ambientale;
- ⇒ i criteri organizzativi per:
 - individuare le modalità per definire le fonti normative accreditate;
 - individuare correttamente gli scenari legislativi applicabili;
 - individuare opportuni canali informativi per assicurare la disponibilità della normativa applicabile alle parti interessate;
 - monitorare il rispetto della normativa applicabile.

Con riferimento alla gestione della documentazione, siano definiti:

- ⇒ i ruoli e le responsabilità nella gestione della documentazione (es. Manuale, Procedure, Istruzioni operative), in coerenza con la politica aziendale;
- ⇒ le modalità di registrazione, gestione, archiviazione e conservazione della documentazione prodotta (es. modalità di archiviazione e di protocollazione dei documenti, a garanzia di adeguata tracciabilità e verificabilità);
- ⇒ i criteri organizzativi per:
 1. predisporre, verificare e emettere documenti connessi con la gestione dell'ambiente, tra cui le procedure e le istruzioni operative;
 2. gestire l'archiviazione e la tracciabilità della documentazione di origine interna ed esterna

È fatto esplicito divieto ai soggetti che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione dei rifiuti, di:

- ⇒ falsificare il registro di carico e scarico rifiuti modificando le reali tempistiche di carico;
- ⇒ gestire i rifiuti in modo difforme da come esplicitato nel presente protocollo, con particolare riferimento al trasporto di rifiuti effettuato in conto proprio in assenza di necessaria autorizzazione;
- ⇒ omettere di archiviare e conservare i documenti.

Gli elementi propri del Modello 231 cui **S.I.O.S.S.** deve porre maggiore attenzione nella definizione del controllo operativo della gestione ambientale, sono:

- la definizione di modalità operative che disciplinano ruoli e responsabilità per la gestione di specifici aspetti ambientali;
- la separazione di poteri e di attività tra i soggetti incaricati di attuare le direttive e quelli deputati al controllo;
- il coinvolgimento, anche tramite flussi informativi, di più soggetti aziendali nelle decisioni in materia di gestione ambientale;
- l'utilizzo di sistemi di registrazione degli adempimenti operativi e di verifica periodica della loro evasione;
- l'esistenza di un sistema di procure e deleghe di funzione in materia ambientale tali da garantire poteri decisionali coerenti con le deleghe assunte, ovvero di un "obbligo di rendicontazione formalizzata sui poteri delegati con modalità prestabilite atte a garantire un'attività di vigilanza senza interferenze"

4.7. Gestione della Salute e Sicurezza sui Luoghi di Lavoro

Responsabile di processo: RSPP, AGQ - Responsabile sistemi di Gestione

Elementi di controllo

S.I.O.S.S. ha la certificazione ISO 45001, perciò tutta la gestione della sicurezza avviene mediante procedure ed istruzioni operative validate da ente terzo.

L'azienda ha articolato la propria organizzazione aziendale per la sicurezza e la salute sui luoghi di lavoro con le figure di seguito indicate:

- **Datore di lavoro (DL):** è stato individuato in qualità di Datore di Lavoro il Sig. Maurizio Puntin cui sono stati conferiti adeguati poteri organizzativi e di spesa ai fini della tutela della salute e sicurezza sul lavoro del personale aziendale;
- **Responsabile del Servizio Prevenzione e Protezione (RSPP):** il Datore di Lavoro, ai sensi della Normativa vigente, anche consultando il Rappresentante dei Lavoratori, ha nominato, previa verifica circa il possesso dei requisiti previsti dalla Normativa vigente, il Responsabile del Servizio di Prevenzione e Protezione esterno all'azienda;
- **Medico Competente (MC)** nominato dal datore di lavoro;
- **Incaricati alle emergenze:** l'individuazione degli incaricati alle emergenze (squadre antincendio e primo soccorso) è stata definita mediante lettera di incarico previa verifica di assenza di eventuali fattori ostativi, del possesso di specifici requisiti (anche in termini di copertura di turni di lavoro e localizzazione) e dell'avvenuta formazione in accordo alle disposizioni legislative in materia;
- **Rappresentante dei lavoratori per la sicurezza (RLS):** nominato dai lavoratori ai sensi della Normativa vigente.

Il Datore di Lavoro è tenuto a vigilare sull'attività svolta dai loro Delegati, attraverso la definizione di opportune reportistiche oggetto di comunicazione periodica da parte dei Soggetti vigilati.

Elementi di controllo della pianificazione:

- è stabilita e comunicata, da parte della Direzione, a tutto il personale ed alle parti interessate, la Politica dell'Azienda - ovvero gli indirizzi e gli obiettivi generali che **S.I.O.S.S.** si prefigge di raggiungere - in materia di Salute e Sicurezza sul Lavoro;
- è assicurata da parte del Datore di Lavoro, in collaborazione con il RSPP, il MC, il RLS - in accordo alla Normativa vigente - la valutazione documentata di tutti i rischi presenti nel perimetro dell'Azienda e delle attività svolte dai lavoratori, nonché la definizione ed attuazione delle procedure di prevenzione e protezione da adottare per eliminare o mitigare il più possibile i rischi evidenziati;
- il Datore di Lavoro assicura inoltre in collaborazione con il RSPP ed il MC:
 - o la definizione di un Budget annuale specifico per la Sicurezza sul Lavoro;
 - o la definizione, per ogni funzione aziendale rilevante, di obiettivi e programmi di miglioramento dei livelli di salute e sicurezza dei lavoratori;

- l'identificazione, l'aggiornamento ed il riesame periodico di tutti i requisiti di legge applicabili all'Azienda in materia di Sicurezza sul Lavoro, quindi l'attuazione delle azioni necessarie al raggiungimento della conformità a detti requisiti;

vige l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, all'Organismo di Vigilanza.

Elementi di controllo per l'attuazione ed il funzionamento

Il Datore di Lavoro assicura, nel rispetto della Normativa vigente ed in collaborazione con il RSPP ed il MC:

- l'informazione, la formazione e l'addestramento del personale aziendale a tutti i livelli ed in relazione alla mansione svolta, anche attraverso la verifica di apprendimento e di efficacia del modello formativo adottato;
- la partecipazione e consultazione dei lavoratori, anche nell'ambito delle riunioni periodiche previste dalla Normativa vigente e per il tramite del loro Rappresentante, nelle diverse attività del Sistema di gestione;
- la programmazione e gestione delle visite mediche e, più in generale, della sorveglianza sanitaria;
- in relazione ai fornitori, appaltatori e contrattisti, in caso di lavori, servizi e forniture:
 - la verifica dell'idoneità tecnico professionale, della congruità dei costi non soggetti a ribasso relativi alla sicurezza, la valutazione dei rischi da interferenza attraverso l'elaborazione del DUVRI;
 - la presenza nei contratti di appalto/fornitura di specifiche clausole di risoluzione e sanzionatorie in caso di violazione/omissione del rispetto dei requisiti Normativi a loro applicabili o imposti dall'Azienda.
- l'adeguatezza e integrità degli asset aziendali attraverso periodiche verifiche manutentive e di conformità ad opera di personale qualificato e idoneo;
- la gestione tempestiva degli incidenti e delle emergenze attraverso la predisposizione e la verifica di efficacia di opportuni piani di emergenza e di gestione del rischio incendio.

Elementi di controllo per la verifica e le azioni correttive

Il Datore di Lavoro assicura, nel rispetto della Normativa vigente in collaborazione con il RSPP ed il MC:

- la costante registrazione, la misura ed il monitoraggio periodico delle performance degli elementi del Sistema Sicurezza, tra cui il grado di conseguimento degli obiettivi di miglioramento, l'efficacia dei controlli definiti, i dati riguardanti le malattie professionali, gli incidenti e la sicurezza degli impianti (impianti elettrici, impianti di messa a terra etc.);
- l'analisi degli infortuni/incidenti e delle malattie professionali al fine di identificarne le possibili cause, quindi definire le opportune azioni correttive, preventive e di miglioramento continuo;
- la gestione delle Non Conformità del Sistema, attraverso la loro identificazione, l'analisi delle cause e la definizione delle opportune azioni correttive/preventive.

5. ORGANISMO DI VIGILANZA (OdV)

Il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è affidato all'Organismo di Vigilanza. Si rinvia al capitolo 7 della parte Generale del Modello Organizzativo Aziendale (MOG).

6. CODICE ETICO

Il Codice etico è il documento ufficiale elaborato da **S.I.O.S.S.** che contiene l'insieme dei fondamenti etici, dei diritti, dei doveri e delle responsabilità dell'organizzazione, nei confronti dei "portatori d'interesse" (dipendenti, fornitori, collaboratori, ecc.). Per quanto riguarda **S.I.O.S.S.** si fa riferimento al testo del Codice etico pubblicato sul sito aziendale, disponibile on-line.

7. SISTEMA SANZIONATORIO

Per quanto riguarda il sistema sanzionatorio, si rinvia allo specifico protocollo disciplinare.

8. RIESAME DEL SISTEMA

Salvo indicazioni diverse da parte dell'OdV, la Direzione provvede al riesame del presente Modello Organizzativo e di Gestione, sulla base dei dati di Audit di sistema per l'anno in corso e di altri dati acquisiti pertinenti con la gestione del sistema. Per tale attività può essere richiesto il supporto dell'OdV.

In particolare, la Direzione esamina e discute non conformità rilevate dall'OdV, al fine di valutare attentamente l'efficacia complessiva del Modello, anche sulla base degli indicatori prestazionali di sistema (vedi paragrafo seguente). Valuta le proposte di aggiornamento e/o integrazione del Modello stesso, indicate dall'OdV e/o dagli altri partecipanti al riesame, pianificando commisurate attività di miglioramento.

9. RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI

Ogni documento previsto nell'ambito del presente Modello organizzativo e di gestione è conservato presso la sede di **S.I.O.S.S.** in un luogo stabilito, a disposizione dell'OdV e di eventuali organi di controllo esterni. Il data base delle informazioni potrà essere memorizzato sia su supporto cartaceo sia magnetico (files) e sarà conservato in archivio.

L'accesso diretto ai documenti, oltre che all'OdV, sarà consentito esclusivamente all'Amministratore Unico e ed al referente aziendale per la 231, tranne i casi in cui siano specificatamente autorizzati altri soggetti.