

1. INTRODUZIONE

Gentile Cittadino,

il documento che sta leggendo è la **Carta dei Servizi** della società **So.Ge.R.T. S.p.a.** (di seguito per brevità denominata **SO.GE.R.T.**), Concessionaria di diversi Comuni per l’Affidamento del servizio di gestione e riscossione volontaria e coattiva delle entrate tributarie comunali: ICP, DPA, TOSAP, IMU, TARI, TASI, EXTRATRIBUTARIE, PATRIMONIALI ED ASSIMILABILI.

Tale documento è stato predisposto secondo le indicazioni della Direttiva del Presidente del Consiglio dei Ministri n. 4/2010, nell’ambito della più generale riforma e modernizzazione dei rapporti fra le Istituzioni e i Cittadini.

Con la Carta Servizi, documento facente parte del sistema di Qualità della società, certificata secondo la norma ISO 9001:2015, **SO.GE.R.T.** conferma l’impegno a promuovere le relazioni con il Cittadino al fine di agevolarlo nell’adempimento degli obblighi tributari, instaurando un rapporto ispirato a criteri di fiducia, collaborazione e trasparenza.

La Carta dei Servizi non è un semplice opuscolo informativo, ma consente al Cittadino di conoscere i servizi e le modalità di erogazione al fine di poter esercitare consapevolmente i propri diritti ed adempiere ai propri obblighi; è inoltre uno strumento per valutare, nel tempo, il nostro operato e promuovere le necessarie iniziative di miglioramento continuo al fine di rendere il nostro servizio sempre più flessibile e vicino al Cittadino.

Per questo motivo La invitiamo a prendere visione dei contenuti del presente documento, offrendoci eventuali Suoi consigli e reclami che saranno considerati come strumenti preziosi al fine di ottimizzare la qualità dei servizi resi.

Si resta a disposizione per ogni Sua richiesta di chiarimento.

1.1 Chi è SO.GE.R.T.

SO.GE.R.T. è una società specializzata nella riscossione delle entrate degli Enti Locali e nelle attività connesse e complementari, da **oltre 30 anni**.

La società è **iscritta al n. 55 dell’Albo** dei soggetti abilitati alla riscossione, liquidazione e accertamento dei tributi e delle entrate degli Enti Locali, istituito presso il Ministero dell’Economia edelle Finanze, ai sensi dell’art. 53 del D.Lgs. n. 446/1997 ed ha un capitale sociale interamente versato pari ad € 10.000.000,00.

La società nasce svolgendo il servizio di tesoreria e riscossione delle entrate patrimoniali degli Enti Pubblici fin dagli anni 90.

Negli anni, per rispondere in maniera sempre più efficace alle esigenze dei Comuni e degli altri Enti Locali, **SO.GE.R.T.** ha sviluppato e potenziato ulteriormente la propria gamma delle attività offerte, nell’ambito delle altre entrate degli Enti Locali (ICI/IMU/TASI, TARSU/TIA/TARES/TARI, Illuminazione votiva, Sanzioni per Violazioni al Codice della Strada, ect.) e dei servizi connessi e complementari, tra cui in particolare quello della Riscossione Coattiva.

1.2 Le Funzioni di SO.GE.R.T.

SO.GE.R.T., nella sua qualità di Concessionario, provvede alla gestione e riscossione (ordinaria, accertamenti, coattiva) dei tributi locali..

1.3 Obiettivi e mission Aziendali

I valori cui **SO.GE.R.T.** ispira la propria attività sono:

- impegno nell'assistenza ed informazione al Cittadino;
- comunicazione chiara ed esaustiva;
- utilizzo ed integrazioni delle più moderne tecnologie;
- affidabilità e professionalità, intese a conquistare la fiducia dei Contribuenti;
- tempestività nel dare risposte alle esigenze dei Contribuenti;
- facilità di accesso ai servizi.

Tutto il processo punta al raggiungimento della “qualità globale” e della gestione in “tempo reale” di tutte le operazioni connesse all'espletamento dell'accertamento, liquidazione e riscossione anche coattiva di tutte le entrate degli Enti Locali, sia di natura tributaria che patrimoniale.

Ciò significa che, ogni operazione è costantemente supervisionata e realizzata con le migliori tecnologie che il mercato possa offrire, al fine di ottenere e rendere un servizio ottimale sia all'Amministrazione Comunale che a tutta la cittadinanza.

1.4 Gli standard e gli impegni di qualità

Per garantire un'alta qualità dei servizi erogati, **SO.GE.R.T.** ha individuato gli aspetti più importanti delle attività svolte misurandole attraverso determinati “**fattori di qualità**” (standard), verificabili d'aparte degli Utenti.

Fattori di qualità	Indicatori
Tempestività degli aggiornamenti normativi degli operatori	☐ <i>Abbonamenti a riviste e quotidiani di settore;</i> ☐ <i>Rassegna stampa on-line</i>
Formazione degli operatori	☐ <i>Corsi di formazione e aggiornamento al Personale</i>
Organizzazione generale	☐ <i>Numero di reclami ricevuti</i>
Informazione del Contribuente	☐ <i>Mezzi di comunicazione diretti e indiretti</i>
Disponibilità degli operatori	☐ <i>Disponibilità all'ascolto;</i> ☐ <i>Comportamento rispettoso e garbato;</i> ☐ <i>Fornitura di risposte esaurienti</i>
Semplificazione	☐ <i>Modulistica disponibile on-line;</i> ☐ <i>Possibilità di invio documentazione on-line</i>
Soddisfazione del Cittadino-Contribuente	☐ <i>Utilizzo di questionari di Customer Satisfaction;</i> ☐ <i>Rilevazione e monitoraggio periodici del grado di soddisfazione</i>

2. IL RAPPORTO CON I CITTADINI

2.1 L'informazione e l'ascolto

L'ascolto dei Cittadini/Contribuenti è un impegno prioritario sia dell'Amministrazione Comunale che del concessionario **SO.GE.R.T.**

Per consentire lo sviluppo della cultura del miglioramento continuo della qualità dei servizi offerti e per incentivare la capacità di dialogo e relazione tra chi eroga la prestazione e chi la riceve, **SO.GE.R.T.** istituirà per conto del Comune di riferimento diverse forme di ascolto del Cittadino/Contribuente:

- **Rilevazioni di soddisfazione** dell'utenza, per verificare il gradimento del servizio prestato.
- **Analisi dei suggerimenti** e delle segnalazioni.
- **Verifica del rispetto degli standard** contenuti nella Carta dei Servizi.

2.2 La valutazione del servizio da parte dei contribuenti

Per garantire un monitoraggio costante del servizio svolto dagli operatori, potranno essere predisposti, di concerto con gli Enti, dei **questionari a risposta multipla**, con livelli di soddisfazione – da insufficiente a buono – su n. 5 aspetti di qualità.

Attraverso tali questionari potrà essere data la possibilità all'Utente di effettuare delle segnalazioni o critiche e di esprimere dei suggerimenti per il miglioramento continuo della qualità del servizio erogato.

Saranno pubblicati sul sito internet www.sogertspa.it dei moduli in forma elettronica.

Presso la sede del comune di riferimento sarà possibile, in forma del tutto anonima, depositare il questionario in appositi contenitori, che a seguire verranno raccolti ed analizzati dal Responsabile per un'analisi trimestrale del grado di soddisfazione dell'utenza. Tali dati saranno, quindi, trasmessi anche all'Amministrazione Comunale per l'accertamento del livello di “*customer satisfaction*” dell'utenza. I risultati delle indagini rappresentano utili indicazioni per impostare i piani di miglioramento del servizio.

2.3 Reclami, Proposte e Suggerimenti

Ogni Utente può presentare reclami o inoltrare suggerimenti relativamente all'erogazione del servizio, con particolare riferimento a quanto disposto dalla presente Carta.

Al fine di agevolare l'Utente, il modulo di presentazione dei reclami/suggerimenti, è reso disponibile presso tutti gli sportelli di **SO.GE.R.T.** ed è, inoltre, scaricabile anche dal sito www.sogertspa.it.

Il reclamo dovrà essere presentato, in forma scritta, mediante consegna diretta agli sportelli **SO.GE.R.T.**, per posta, via fax o per posta elettronica. Per ottenere una risposta il modulo dovrà contenere le generalità della persona che lo ha redatto, con indirizzo ed eventuale numero di telefono e la sua firma. L'eventuale presentazione informale (verbale diretta o telefonica) sarà considerata in ogni caso, ma alla stregua di semplice segnalazione alla quale non verrà, tuttavia, data risposta.

Oltre ai reclami gli Utenti possono presentare, con le medesime modalità, proposte di miglioramento dei servizi e suggerimenti in merito agli stessi.

In caso di presentazione formale, il responsabile di servizio di **SO.GE.R.T.** valuta il reclamo e risponde all'Utente con la massima celerità e comunque entro **30 giorni** lavorativi dalla presentazione dello stesso. Nel caso di particolari richieste che comportino una approfondita analisi, entro tale termine sarà comunque inviata al Cittadino una lettera, nella quale si spiegano le ragioni della necessità di proroga per l'espletamento dell'intera pratica, stabilendo un ulteriore termine.

Se il reclamo è riconosciuto fondato saranno adottati i provvedimenti più opportuni per eliminare il disservizio segnalato.

I reclami ed i suggerimenti ricevuti vengono raccolti in un report annuale e di essi si tiene conto al fine della redazione del piano di miglioramento della qualità.

I reclami ed i suggerimenti dei Contribuenti sono strumenti preziosi per ottimizzare la qualità dei servizi di SO.GE.R.T.

3. LA GARANZIA E LA TUTELA DEI CONTRIBUENTI

Anche la SO.GE.R.T. si ispira ai principi generali fissati dallo "Statuto dei diritti del contribuente" (Legge n. 212/2000, modificata dal D.Lgs n. 32/2001) Diritto all'informazione.

4. DIRITTO ALL'INFORMAZIONE

Si assicura la conoscenza delle leggi, dei regolamenti e delle disposizioni in materia fiscale e la diffusione tempestiva ed efficace degli atti di nuova emanazione.

5. DIRITTO ALLA CHIAREZZA E ALLA MOTIVAZIONE DEGLI ATTI

Al fine di assicurare maggiore chiarezza e trasparenza, tutti gli atti di riscossione coattiva devono essere motivati.

6. L'AUTOTUTELA

Tale istituto si sostanzia nel potere – dovere di rimuovere o modificare atti precedentemente emanati e ritenuti illegittimi ed infondati.

Il potere di annullamento dell'atto, o di rinuncia all'imposizione, sorge in tutti i casi di illegittimità dell'atto o dell'imposizione, come ad esempio nelle ipotesi di:

- errore di persona;
- evidente errore logico o di calcolo;
- errore sul presupposto dell'imposta;
- doppia imposizione;
- mancata considerazione di pagamenti regolarmente eseguiti;
- mancanza di documentazione successivamente sanata (non oltre i termini di decadenza);
- difetto di notifica.

L'annullamento può essere effettuato anche se è pendente il giudizio o se l'atto è divenuto ormai definitivo per decorso dei termini per ricorrere e anche se il contribuente ha presentato ricorso e questo è stato respinto per motivi formali con sentenza passata in giudicato. Non è consentito solo

in presenza di un giudicato di merito favorevole all'amministrazione. L'annullamento dell'atto illegittimo comporta automaticamente l'annullamento degli atti ad esso consequenziali (ad es. il ritiro di un avviso di accertamento infondato comporta l'annullamento della conseguente ingiunzione fiscale) e l'obbligo di restituzione delle somme indebitamente riscosse.

7. ACCESSO AGLI ATTI

L'accesso agli atti è il diritto riconosciuto ai singoli cittadini, alle imprese e alle associazioni, di prendere visione di un documento amministrativo e di ottenerne copia.

Favorisce la partecipazione all'attività amministrativa e ne assicura l'imparzialità e la trasparenza. E' prevista dalla Legge 241 del 1990, regolamentata dal D.P.R. 352 del 1992 e modificata dalle leggi 11 febbraio 2005, n.15 e 14 maggio 2005, n.80.

Si può esercitare nei confronti di enti e amministrazioni pubbliche (i ministeri, le scuole, le università, le regioni, le A.S.L.), ma anche di gestori di servizi pubblici

8. INFORMAZIONI UTILI

8.1 Ubicazione Ufficio

Per ciascun comune di riferimento è allestito un ufficio front office o telematico, a seconda delle esigenze. Contestualmente sono attive linee telefoniche (anche numero verde) e mail specifiche per tutte le esigenze di contatto dei contribuenti.

8.2 Lo sportello dedicato

Con il fine di rispondere all'esigenza di offrire ai contribuenti appartenenti a particolari categorie priorità di trattamento durante le attese agli sportelli presenti sul territorio nazionale, la Società ha attivato lo sportello dedicato a soggetti portatori di handicap, anziani, invalidi e donne in stato di gravidanza.

8.3 Consigli ai cittadini

Il sito internet della Società è costantemente aggiornato: non esitate a consultarlo per usufruire dei servizi telematici, ottenere aggiornamenti normativi e scaricare la modulistica che vi occorre.

Prima di recarsi presso gli sportelli è bene controllare di essere in possesso di tutta la documentazione necessaria a definire la pratica.

8.4 Modalità di pagamento

I pagamenti possono essere effettuati:

- Versamento con bollettino C.C.P.
- Bonifico postale
- Altri sistemi di pagamento previsti e resi obbligatori dalle vigenti normative.



SO.GE.R.T. S.P.A.

CODICE ETICO

EX ART.6, COMMA 3,

D.LGS. 8 GIUGNO 2001 N. 231

aggiornato al 13 maggio 2022

INDICE

1	Finalità	3
1.2	Definizioni	4
1.3	SO.GE.R.T. S.p.A.: valori e principi generali	5
1.4	I valori su cui si fonda l'attività di SO.GE.R.T. S.p.A	6
1.5	Adozione e diffusione del Codice Etico	9
1.6	Aggiornamento	10
1.7	Applicabilità	10
1.8	Obblighi dei Destinatari	11
1.9	Obiettivi gestionali e conformità alle regole	11
1.10	Corporate Governance e attività dell'azienda	12
2	Regole di comportamento	13
2.1	Rapporti con i contribuenti	13
2.2	Rapporti con dipendenti e collaboratori	13
2.3	Relazioni con i Consulenti e Fornitori dell'azienda	14
2.4	Relazioni con i partner d'affari e le altre controparti contrattuali	15
2.5	Relazioni con la Pubblica Amministrazione, comunità locali e istituzioni pubbliche	16
2.6	Rapporti con i mass media	17
2.7	Partecipazione a procedure di gara indette dalla Pubblica Amministrazione	18
2.8	Richiesta di fondi pubblici e loro gestione	18
2.9	Partecipazione a procedimenti giudiziari	19
2.10	Relazioni con partiti politici, organizzazioni sindacali e associazioni portatrici di interessi	20
2.11	Rapporti con le Autorità di Vigilanza e Controllo	21
2.12	Rapporti con il Collegio Sindacale, le Società di revisione e altre strutture	21
2.13	Informazioni riservate e protezione dei dati personali	21
2.14	Doni, benefici o altre utilità	22
2.15	Utilizzo di attrezzature, dispositivi e strutture aziendali	23
2.16	Registrazioni contabili	23
3.	Risorse umane	24

3.1	Conflitto di interessi e attività lavorativa esterna da parte dei dipendenti	25
4.	Ambiente	25
5.	Salute e Sicurezza sul lavoro	26
6.	Remunerazione	29
7.	Attività collaterali	29
8.	Prevenzione	29
9.	Controlli	30
10.	Sanzioni	30
11.	Segnalazioni	31

1 Finalità

Il Codice Etico insieme al Modello Organizzativo, costituisce elemento essenziale per contribuire alla prevenzione e alla repressione dei reati all'interno delle compagini aziendali. E' uno strumento per la disciplina e l'attuazione di buone pratiche di comportamento, un punto di riferimento e una guida per chi lavora in SO.GE.R.T. S.p.A. e per chi ha interesse a perseguirne la missione

Esprime impegni e responsabilità che chi lavora in SO.GE.R.T. S.p.A., ovvero con essa venga in contatto, si assume nel condurre ogni attività aziendale.

Mentre per quanto riguarda i comportamenti legalmente illegittimi la casistica è completa (sono le leggi e i contratti che li definiscono), essa lo è molto meno per quelli eticamente illegittimi, o opportunistici.

L'opportunistista sfrutta a suo vantaggio le incompletezze (o le parti meno chiare) del contratto o della norma contando sulle difficoltà a controllare se egli ne abbia sino in fondo rispettato lo spirito. Si tratta dunque dei casi in cui il comportamento legittimo non è individuabile di primo acchito, proprio perché la legge o il contratto non possiedono sufficiente finezza analitica o normativa. Un comportamento opportunistico non è dunque necessariamente illegale: possono esistere comportamenti legali che prevedono qualche forma di sfruttamento da parte di determinate categorie di soggetti a danno di altre, o che possono recare offesa a qualcuno o a beni tutelati

Ecco che diviene necessario, al fine di orientare e giudicare i comportamenti, "*aggiungere finezza*" alla strumentazione normativa in essere, identificando i casi ("*fattispecie e contingenze*") in cui possono manifestarsi i comportamenti inaccettabili secondo una metrica morale condivisa, seppure non sempre specificamente normata.

Bisogna infine notare che i comportamenti opportunistici – non dichiaratamente illegali, ma contrari all'etica dell'organizzazione o all'etica sociale – sono quelli da cui dipende, benché in parte, l'immagine di una organizzazione. Esiste dunque, alla fine, un diretto rapporto tra rispetto delle regole e autorevolezza, affidabilità e dunque successo dell'impresa.

1.1 Utilità

Il Codice serve innanzitutto a definire l'ammissibilità o inammissibilità dei comportamenti e ad impegnare l'utenza al rispetto dei principi ivi esplicitati, ma esso contiene anche altri obiettivi:

- a) l'aumento di coesione e di coerenza del sistema: il codice ha come scopo il miglioramento delle relazioni interne e la formazione di una immagine esterna unitaria e chiara;
- b) la maggiore efficienza dell'organizzazione: l'abolizione dei comportamenti opportunistici e la motivazione del massimo numero dei partecipanti verso obiettivi positivi aumentano la capacità di produrre utilità, sia per i più diretti interessati sia per l'ambiente di riferimento nel suo complesso;
- c) una buona reputazione: una organizzazione con buone regole, che manifesta in maniera univoca i suoi valori, che in modo trasparente sia in grado di individuare i comportamenti ritenuti negativi e di rendere pubblico l'apprezzamento per i comportamenti positivi, produce sicurezza nei soggetti con cui ha che fare, i quali si trasformano, a seconda degli interessi presenti, da interlocutori a *partner*.

Un'ultima notazione riguarda la natura protettiva del Codice Etico: esso non è principalmente uno strumento rivolto a sanzionare, ma ad indurre e indirizzare.

Un protocollo che aiuti i suoi destinatari ad affrontare i dilemmi etici che si presentano nell'attività di tutti i giorni.

L'organismo di controllo che verifica la sua applicazione, più che come un istituto giudicante, deve dunque essere inteso come una entità di promozione e di sviluppo dei comportamenti positivi.

1.2 Definizioni

Codice: il presente Codice nella versione vigente e gli eventuali allegati.

Decreto: il decreto legislativo 8 giugno 2001, n. 231, recante *“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”*, e

successive integrazioni e modificazioni.

Società: SO.GE.R.T. S.p.A., con sede a Grumo Nevano (NA), Piazza Cirillo, n. 5.

Destinatari: i soggetti ai quali si applicano le disposizioni del Codice, tra i quali gli Esponenti Aziendali, i Dipendenti, i Collaboratori, nonché le persone che, intrattenendo rapporti con la Società, si impegnano all'osservanza del Codice.

Esponenti Aziendali: il Presidente, i componenti del Consiglio di Amministrazione e del Collegio sindacale, i componenti degli altri organi della Società eventualmente istituiti ai sensi dell'art. 2380 codice civile o delle leggi speciali, nonché qualsiasi altro soggetto in posizione apicale ai sensi del Decreto, per tale intendendosi qualsiasi persona che rivesta funzioni di rappresentanza, amministrazione o direzione dell'azienda o di una unità o divisione di questo, dotato di autonomia finanziaria e funzionale.

Dipendenti: i soggetti che intrattengono con la società un rapporto di lavoro subordinato, inclusi i lavoratori a termine compresi quelli con contratto di inserimento o di apprendistato o a tempo parziale, nonché i lavoratori in distacco ovvero in forza con contratti di lavoro para-subordinato (somministrazione di lavoro).

Collaboratori: i soggetti che intrattengono con l'azienda: (i) rapporti di lavoro a progetto; (ii) rapporti di agenzia e altri rapporti che si concretino in una prestazione di opera coordinata e continuativa, prevalentemente personale, a carattere non subordinato; (iii) rapporti di collaborazione occasionale, nonché i soggetti sottoposti alla direzione o vigilanza di un Esponente Aziendale.

Organismo di Vigilanza: l'organismo di vigilanza previsto dall'art. 6 del Decreto legislativo.

1.3 SO.GE.R.T. S.p.A.: valori e principi generali

In piena sintonia con le posizioni espresse e tutelate dal sistema associativo al quale aderisce, la SO.GE.R.T. S.p.A. è consapevole di contribuire con il proprio operato, con senso di responsabilità ed integrità morale, al processo di sviluppo dell'economia italiana ed alla crescita civile e sociale del Paese.

L'azienda crede nel valore del lavoro e considera la legalità, la correttezza e la trasparenza dell'agire presupposti imprescindibili per il raggiungimento dei propri obiettivi economici, produttivi, sociali.

La SO.GE.R.T. S.p.A., la cui attività si svolge quotidianamente sotto gli occhi di tutti i cittadini, basa la sua organizzazione su valori come la trasparenza, credibilità e chiarezza.

L'Azienda persegue il livello di prestazioni volto alla piena soddisfazione dei propri interlocutori, inquadrando tutte le iniziative in un'ottica di sviluppo sostenibile, perseguendo sempre obiettivi di crescita e di ampliamento della gamma di prodotti da offrire ai contribuenti.

Nelle proprie attività, SO.GE.R.T. S.p.A. ha identificato alcuni valori di riferimento che orientano i comportamenti di tutte le persone che agiscono per suo conto, al fine di assicurare la correttezza nella conduzione dell'attività della società, a tutela del patrimonio e dell'immagine dello stesso e delle aspettative di tutti gli interlocutori di riferimento.

Attraverso l'adozione del Codice Etico, SO.GE.R.T. S.p.A. individua l'insieme delle regole:

- di comportamento nei rapporti con gli interlocutori esterni, i collaboratori, il mercato e l'ambiente, alle quali l'Azienda uniforma la propria attività interna ed esterna, esigendone il rispetto da parte di tutti i collaboratori, i consulenti e, per quanto di competenza, gli interlocutori esterni;
- di organizzazione e gestione dell'Azienda, finalizzate alla realizzazione di un sistema efficiente ed efficace di programmazione, esecuzione e controllo delle attività tale da assicurare il costante rispetto delle regole di comportamento e prevenirne la violazione da parte di qualsiasi soggetto che operi per l'Azienda.

Nello svolgimento della propria attività, l'azienda rispetta le leggi, i regolamenti, le procedure aziendali e le norme di autodisciplina, nonché i valori e i principi dell'Etica.

1.4 I valori su cui si fonda l'attività di SO.GE.R.T. S.p.A.

Il Codice contiene i principi e le regole etiche fondamentali che devono orientare le condotte di tutti coloro che operano nell'azienda, affinché qualsiasi loro comportamento – all'interno dell'azienda e nei confronti di terzi, in primo luogo i contribuenti, i fornitori e gli organi istituzionali – sia conforme, oltre che alla legge, ai principi di onestà, correttezza, fedeltà, lealtà, trasparenza, imparzialità e riservatezza.

- **Onestà**

SO.GE.R.T. S.p.A., ha come principio imprescindibile il rispetto delle Leggi e dei Regolamenti, dei Contratti di lavoro di qualsiasi livello, degli accordi vincolanti per Statuto.

Nell'ambito della loro attività professionale, i Dipendenti, gli Organi dell'azienda, gli Amministratori, i Consulenti, i collaboratori esterni, i Fornitori, gli Enti pubblici con i quali la Società intrattiene rapporti e chiunque collabori o abbia un qualsiasi rapporto con la SO.GE.R.T. S.p.A., sono tenuti ad osservare con diligenza le Leggi e i regolamenti vigenti nonché quanto previsto dallo Statuto.

In nessuna circostanza il perseguimento dell'interesse dell'azienda può giustificare una condotta non onesta.

SO.GE.R.T. S.p.A. non inizierà o proseguirà nessun rapporto con chi non intenda allinearsi a questo principio.

SO.GE.R.T. S.p.A. non tollera e non tollererà i coinvolgimenti dei dipendenti in una qualsiasi forma di comportamento illegale. In particolar modo i dipendenti ed i componenti degli Organi dell'Azienda devono essere a conoscenza delle leggi e dei regolamenti da queste discendenti; qualora sussistessero dubbi su come procedere nell'ambito della loro attività, possono chiedere chiarimenti alla Direzione dell'azienda ovvero all'Organismo di Vigilanza qualora questi dubbi permangano.

Ai dipendenti ed ai componenti degli Organi dell'azienda è vietato svolgere attività o assumere comportamenti che potrebbero sollevare interrogativi sull'integrità, l'imparzialità o la reputazione di SO.GE.R.T. S.p.A.; questo impone non soltanto agire in modo etico, ma anche rendere evidente a terzi questo principio.

- **Correttezza**

Nell'esercizio di ogni attività devono essere sempre evitate situazioni, anche solo potenziali, di conflitto di interesse, ossia situazioni in cui un dipendente, un Membro di un Organo dell'Azienda, un Consulente, un Fornitore o un Collaboratore esterno, direttamente e/o indirettamente, sia portatore di un interesse personale che potrebbe interferire con i doveri verso l'Azienda.

E' richiesto a tutti i dipendenti, nel rispetto dei principi dello Statuto dei Lavoratori e senza che essi siano identificabili come atteggiamenti delatori, di riportare all'Azienda tutti i casi conosciuti

o supposti di conflitto di interesse relativamente a se stessi, a colleghi, fornitori od altri soggetti comunque legati alla Società.

- **Lealtà**

L'azienda considera la lealtà un principio fondamentale. In questo senso si impegna a:

- non sfruttare condizioni di ignoranza o di incapacità (anche solo temporanea);
- evitare che, nei rapporti in essere, chiunque operi a suo nome e per suo conto tenti di trarre vantaggio da lacune contrattuali o eventi imprevisti di vario genere con l'obiettivo di sfruttare la posizione di dipendenza o debolezza nelle quali si sia venuto a trovare l'interlocutore. L'azienda intende inoltre tutelare il valore della concorrenza leale e pertanto si astiene da comportamenti di tipo collusivo o similare.

- **Trasparenza e tracciabilità delle informazioni**

I dipendenti, gli Amministratori e i Collaboratori esterni dell'azienda sono tenuti a dare informazioni complete, trasparenti, veritiere, comprensibili ed accurate, con l'obiettivo di corrispondere alle attese di conoscenza degli impatti economici, sociali e ambientali delle attività aziendali.

In tal modo, nell'impostare i rapporti con l'azienda, chiunque vi entri in contatto deve essere messo nelle condizioni di prendere decisioni autonome e consapevoli.

Ogni operazione dell'azienda deve essere correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua. A tal fine, tutte le azioni e le operazioni dell'azienda devono avere una registrazione adeguata e deve essere possibile la verifica del processo di decisione, autorizzazione e svolgimento.

Per ogni operazione, in particolare quelle relative alle aree sensibili, deve essere pertanto predisposto un adeguato supporto documentale od informatico, al fine di poter procedere in ogni momento, all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha effettuato, registrato e verificato l'operazione stessa.

- **Imparzialità**

L'attività della SO.GE.R.T. S.p.A. deve essere improntata alla massima imparzialità nei confronti di tutti gli interlocutori dell'Azienda.

I criteri di imparzialità e merito per quanto riguarda il personale devono essere applicati nella selezione, retribuzione, formazione progressione delle carriere.

Nello svolgimento della sua attività l'azienda deve assicurare il rispetto delle procedure e un trattamento omogeneo per contribuenti, fornitori, e in genere con tutti i soggetti con cui l'azienda intrattiene rapporti.

- **Riservatezza**

SO.GE.R.T. S.p.A. garantisce la riservatezza delle informazioni in suo possesso. I Dipendenti, gli Amministratori ed i Collaboratori esterni sono tenuti quindi a rispettare le regole stabilite in conformità alla Legge che tutela la riservatezza dei dati personali e sensibili e sono tenuti ad utilizzare le informazioni acquisite in relazione alla propria attività professionale svolta per conto dell'azienda.

Il Documento Programmatico sulla sicurezza, redatto ai sensi della normativa vigente, è disponibile presso gli Uffici della SO.GE.R.T. S.p.A. e deve essere rispettato da chiunque abbia nella propria disponibilità qualsiasi dato dell'azienda.

1.5 Adozione e diffusione del Codice Etico

Il Codice etico, quale parte integrante del Modello di Organizzazione, è adottato dalla SO.GE.R.T. S.p.A. con delibera del Consiglio di Amministrazione.

L'azienda attribuisce la massima importanza al rispetto del Codice Etico da parte di tutti i Destinatari, anche come condizione per la salvaguardia e promozione della sua immagine e reputazione.

Del Codice è data ampia diffusione interna, ed è a disposizione di qualunque interlocutore dell'azienda.

Tutti i Destinatari sono tenuti all'osservanza del Codice Etico. A tal fine l'azienda, anche nel quadro delle attività di formazione ed aggiornamento professionale e nell'esercizio della potestà disciplinare:

- promuove, con azioni continuative ed efficaci, la conoscenza ed il rispetto del Codice ad ogni livello organizzativo;
- verifica, attraverso apposite ed adeguate strutture di vigilanza e presidi documentali, l'osservanza del Codice;

- sanziona adeguatamente le violazioni al Codice.

L'efficacia del Codice alla luce dell'evoluzione normativa e delle *best practices* di settore, nonché dei cambiamenti nell'organizzazione e nell'attività dell'Azienda sono soggette a costante verifica.

1.6 Aggiornamento

Con delibera del Consiglio di Amministrazione il Codice Etico può essere modificato ed integrato, anche sulla scorta dei suggerimenti e delle indicazioni provenienti dall'Organismo di Vigilanza.

1.7 Applicabilità

Il Codice si applica a tutti i Destinatari. Ove necessario, l'azienda rende giuridicamente vincolanti le norme del Codice mediante opportuni atti o negozi giuridici.

I Dipendenti sono tenuti all'osservanza del Codice Etico in base all'art. 2104 cod. civ.

I Destinatari devono informare i terzi degli obblighi sanciti dal Codice e pretenderne il rispetto. I Destinatari hanno l'obbligo di osservare il Codice sia nei rapporti tra loro (c.d. *rapporti interni*), sia nei rapporti con i terzi (c.d. *rapporti esterni*).

In particolare:

- i.* gli organi della SO.GE.R.T. S.p.A., nell'ambito delle loro funzioni, uniformano la propria condotta alle previsioni del Codice, sia all'interno dell'azienda rafforzando così la coesione e lo spirito di reciproca collaborazione, sia nei confronti dei terzi che entrano in contatto con l'azienda;
- ii.* i responsabili di funzioni ed uffici dell'azienda esigono il rispetto del Codice da parte dei Dipendenti e dei Collaboratori e vigilano sul loro comportamento al fine di prevenire violazioni. In particolare, ciascun responsabile ha l'obbligo di:
 - informare i propri collaboratori in maniera chiara, precisa e completa circa i loro obblighi, compreso il rispetto del Codice;
 - comunicare con chiarezza che qualsiasi violazione del Codice è fortemente riprovata e che essa può costituire inadempimento contrattuale e/o illecito disciplinare, salva la previsione del comportamento come illecito penale;

- riferire tempestivamente, tramite informativa scritta, all'Organismo di Vigilanza circa qualsiasi presunta violazione del Codice direttamente accertata o di cui abbia appreso da altri;
 - nell'ambito delle funzioni attribuite, attuare o promuovere l'adozione di misure idonee ad evitare le violazioni del Codice e la loro reiterazione;
 - impedire ritorsioni nei confronti di qualunque Destinatario abbia riferito all'Organismo di Vigilanza e/o ad un responsabile circa presunte violazioni di cui sia venuto a conoscenza, garantendo la segretezza del relativo flusso informativo;
- iii.* il responsabile del processo di selezione e assunzione del personale, effettua un'accurata selezione dei candidati anche sulla base delle loro attitudini personali al rispetto del presente Codice.

1.8 Obblighi dei Destinatari

I Destinatari svolgono le loro funzioni o mansioni con diligenza e con la professionalità richiesta dalla natura di queste, e si conformano ai principi di onestà, correttezza, fedeltà, lealtà, trasparenza, imparzialità e riservatezza.

I Destinatari sono tenuti a rispettare la dignità delle persone e la loro sfera privata, sia nelle relazioni interne che in quelle esterne.

Non sono ammesse né tollerate discriminazioni basate sulla nazionalità, l'origine razziale o etnica, le credenze religiose, il sesso e l'orientamento sessuale, le condizioni di salute o altro, e neppure molestie di qualsiasi natura od offese.

Nell'ambito dello svolgimento di attività gerarchicamente ordinate, i Dipendenti operano con spirito di leale collaborazione, nel rispetto delle regole interne e, più in generale, secondo il principio della correttezza.

1.9 Obiettivi gestionali e conformità alle regole

Gli obiettivi fissati dall'Organo Amministrativo della Società sono perseguiti in conformità allo statuto sociale ed alla normativa applicabile ed ai principi di correttezza operativa e gestionale.

SO.GE.R.T. S.p.A. e tutti i Destinatari devono conformarsi ai più elevati *standard* di eccellenza qualitativa e perseguire l'obiettivo del rafforzamento della reputazione e solidità dell'azienda, della fiducia della clientela e della soddisfazione degli interessi dei soggetti destinatari dei servizi

svolti dalla SO.GE.R.T. S.p.A..

La consapevolezza del ruolo di interesse generale e strategico per l'ambiente, delle attività poste in essere dalla SO.GE.R.T. S.p.A., fa sì che l'azienda si impegni ad operare sempre nel rispetto dello stesso, salvaguardando la qualità e l'integrità dei suoi servizi. Per tutelare questi valori, comuni, condivisi ed irrinunciabili, l'azienda ha messo in atto procedure di controllo idonee ed efficaci.

Il senso di responsabilità, il comportamento e gli atteggiamenti assunti nei confronti degli aspetti dell'azienda relativi alla corretta gestione delle problematiche di salute e di sicurezza costituiscono parte integrante della mansione di ciascun dipendente e sono, pertanto, elemento significativo di giudizio sulle prestazioni di ciascun dipendente e sulla qualità di quelle rese da terzi.

1.10 Corporate Governance e attività dell'azienda

SO.GE.R.T. S.p.A. adotta un sistema di governo conforme a quanto previsto dalla normativa ad essa applicabile.

Gli organi statutari sono:

- Assemblea dei Soci;
- Consiglio di Amministrazione;
- Collegio Sindacale;

Il modello di impresa adottato da SO.GE.R.T. S.p.A. intende perseguire il raggiungimento di un equilibrio che riesca ad integrare l'obiettivo di equilibrio economico-finanziario, con le esigenze e le aspettative dei propri interlocutori, oltre che con il rispetto e la salvaguardia del territorio, dove ha sede la propria azienda.

Le attività e i processi all'interno dell'azienda sono ispirati a principi di trasparenza e di tracciabilità delle decisioni.

A questo scopo, tutte le operazioni devono essere documentate e i documenti conservati in originale (o in copia di cui sia garantita la conformità all'originale), in modo che sia sempre possibile individuare le singole azioni compiute nelle varie fasi che caratterizzano tali operazioni, i relativi autori e, ove enunciate, le motivazioni delle stesse.

Ferme restando al riguardo le norme vigenti o l'autoregolamentazione, le situazioni anche di

potenziale conflitto di interesse devono sempre essere comunicate all'Organismo di Vigilanza e adeguatamente gestite, allo scopo di evitare pregiudizi per la clientela, le controparti o l'azienda. Salvo quanto previsto dall'art. 2391 c.c., quando la situazione di conflitto può comportare il pregiudizio dell'interesse dei contribuenti o dell'azienda, è obbligatoria l'astensione dall'attività da parte del Destinatario titolare dell'interesse extrasociale.

2 Regole di comportamento

2.1 Rapporti con i contribuenti

Si definisce “*contribuente*” della SO.GE.R.T. S.p.A., chiunque fruisca dei servizi dell'impresa a qualunque titolo.

SO.GE.R.T. S.p.A. impronta la relazione con i contribuenti alla disponibilità, al rispetto, alla cortesia e alla partecipazione. SO.GE.R.T. S.p.A. si impegna a informare il contribuente in modo trasparente, tempestivo e completo sulle caratteristiche, funzioni, costi e rischi dei prodotti e servizi offerti.

L'azienda garantisce che il trattamento dei dati personali dei contribuenti avviene nel rispetto della normativa vigente e dell'ispirazione del presente Codice etico.

Garantisce, inoltre, che i dati e le informazioni sono registrati ed elaborati in modo completo, tempestivo e nel rispetto della dovuta riservatezza.

2.2 Rapporti con dipendenti e collaboratori

Si definisce “*dipendente*” e/o “*collaboratore*” chiunque intrattenga con la Società una relazione di lavoro finalizzata al raggiungimento degli scopi dell'impresa.

SO.GE.R.T. S.p.A. garantisce un ambiente di lavoro in cui ciascuno possa collaborare esprimendo la propria attitudine professionale.

L'azienda, nel rapporto di lavoro, valorizza le competenze, le potenzialità e l'impegno, adoperando criteri di valutazione oggettivi.

L'azienda ed i suoi collaboratori devono tenere comportamenti corretti negli affari di interesse della SO.GE.R.T. S.p.A. e nei rapporti con la Pubblica Amministrazione.

Qualsiasi azione diretta ad alterare le condizioni di corretta competizione è contraria alla politica aziendale dell'azienda ed è vietata ad ogni soggetto che per essa agisce.

In nessun caso il perseguimento dell'interesse dell'azienda può giustificare un condotta dei vertici o dei collaboratori dell'azienda che non sia rispettosa delle leggi vigenti e conforme alle regole del presente Codice.

2.3 Relazioni con i Consulenti e Fornitori dell'azienda

Sono "*fornitori*" tutti coloro che, a vario titolo, forniscono beni, servizi, prestazioni e risorse necessari alla realizzazione delle attività e all'erogazione dei servizi, concorrendo al raggiungimento degli obiettivi della Società.

Le relazioni con i fornitori dell'azienda, comprensive dei contratti finanziari e di consulenza, sono regolate dalle norme di questo Codice e sono oggetto di costante ed attento monitoraggio da parte dell'azienda.

La selezione dei Fornitori deve avvenire in maniera trasparente, secondo criteri oggettivi e predeterminati, che tengano conto esclusivamente della professionalità, competenza, affidabilità ed economicità complessiva del Fornitore, in relazione alla natura del bene o del servizio da ottenere.

I rapporti con i Fornitori sono improntati a correttezza e buona fede e devono essere documentati e ricostruibili.

I contratti con i Fornitori devono prevedere come condizione che il Fornitore si impegni al rispetto del Codice; chi intrattiene rapporti con il Fornitore è tenuto a segnalare al responsabile della funzione e/o all'Organismo di Vigilanza inadempienze significative e non conformità rispetto al Codice.

Nessun soggetto dell'azienda o che agisce in suo nome può intrattenere rapporti con alcun Fornitore ove abbia un interesse, anche non patrimoniale o indiretto, nell'attività del medesimo.

Il dipendente non chiede né accetta, per sé o per altri, regali o altre utilità offerti da fornitori.

Omaggi o atti di ospitalità, concessi o ricevuti, previa comunicazione all'Organismo di Vigilanza

sono consentiti solo se di esiguo valore e comunque limitati all'ambito delle normali relazioni di cortesia commerciale.

Le condizioni a cui la fornitura viene effettivamente erogata devono essere quelle pattuite contrattualmente.

2.4 Relazioni con i partner d'affari e le altre controparti contrattuali

Con il termine *partner* d'affari si intendono quei soggetti coinvolti direttamente o indirettamente nell'attività dell'azienda che hanno un qualche interesse in relazione alle decisioni, alle iniziative strategiche e alle possibili azioni svolte dalla Società.

Rientrano, pertanto, tra i *partner* d'affari e le altre parti contrattuali, a titolo meramente esemplificativo, i dipendenti, i contribuenti, gli azionisti, i cittadini, i procuratori, i collaboratori a qualsiasi titolo, i fornitori, i *partner* finanziari e/o commerciali, le istituzioni comunali, provinciali e nazionali, le associazioni di categoria, le associazioni ambientali e, più in generale, chiunque sia portatore di un interesse nei confronti della SO.GE.R.T. S.p.A.

L'azienda instaura rapporti solo con *partner* d'affari e controparti contrattuali che godano di buona reputazione, che siano impegnati solo in attività lecite e la cui cultura etica aziendale sia comparabile a quella dell'azienda.

L'azienda e i Destinatari si astengono dal concludere accordi contrari alla legge, simulati o segreti. La correttezza nei rapporti con tali soggetti è obiettivo irrinunciabile della SO.GE.R.T. S.p.A. e condizione idonea a favorire, tra l'altro:

- la fedeltà e la fiducia dei contribuenti;
- l'affidabilità dei fornitori, dei collaboratori esterni e dei *partner* commerciali;
- il miglioramento continuo dei rapporti con le risorse umane che prestano la propria attività nella Società;
- lo sviluppo di un dialogo virtuoso con le comunità e le istituzioni locali;
- la gestione dei rapporti con la Pubblica Amministrazione improntata a criteri di trasparenza e correttezza;
- la gestione dei rapporti con le Autorità ispirata a criteri di collaborazione, la veridicità e completezza delle informazioni fornite agli organi di stampa;

- evitare e prevenire la commissione di atti illeciti e di reati, con particolare riferimento a quelli previsti dal decreto e successive modifiche e integrazioni.

I rapporti con i *partner* d'affari e le controparti contrattuali in genere sono anch'essi tenuti nel rispetto del Codice. I rapporti in questione sono intrattenuti da soggetti professionalmente preparati e competenti, individuati secondo le norme interne dell'azienda.

I Destinatari segnalano tempestivamente al proprio superiore e/o all'Organismo di Vigilanza ogni comportamento del *partner* d'affari o della controparte contrattuale che appaia in contrasto con il Codice.

2.5 Relazioni con la Pubblica Amministrazione, comunità locali e istituzioni pubbliche

Nelle relazioni con la Pubblica Amministrazione e, in generale, con organismi pubblici, italiani, sovranazionali o esteri l'azienda si attiene scrupolosamente alle previsioni del Codice etico e delle leggi vigenti.

SO.GE.R.T. S.p.A. ed i suoi collaboratori devono tenere comportamenti corretti nella gestione degli interessi dell'azienda e nei rapporti con la Pubblica Amministrazione.

Qualsiasi azione diretta ad alterare le condizioni di corretta competizione è contraria alla politica aziendale della SO.GE.R.T. S.p.A. ed è vietata ad ogni soggetto che agisce per conto della stessa. In nessun caso il perseguimento dell'interesse dell'azienda può giustificare un condotta dei vertici o dei collaboratori dell'azienda che non sia rispettosa delle leggi vigenti e conforme alle regole del presente Codice Etico.

In ogni comunicazione con l'esterno le informazioni riguardanti la SO.GE.R.T. S.p.A. e le sue attività devono essere veritiere, chiare, verificabili.

L'atteggiamento della SO.GE.R.T. S.p.A. nei confronti di tutte le istituzioni deve essere orientato alla trasparenza, al dialogo e alla collaborazione.

SO.GE.R.T. S.p.A., assicura il rispetto delle esigenze del territorio, la costante definizione di uno sviluppo sostenibile delle infrastrutture, la costante ricerca di metodi di erogazione dei prodotti e servizi sempre più coerenti con le esigenze dei contribuenti e con la produttività dell'impresa e sostenibili dal punto di vista ambientale.

Al fine di garantire la massima chiarezza nei rapporti, i contatti con gli interlocutori istituzionali avvengono esclusivamente tramite referenti che abbiano ricevuto esplicito mandato.

Alcuni comportamenti possono essere ritenuti inaccettabili se non addirittura in aperta violazione della legge e/o dei regolamenti, se tenuti nei confronti di dipendenti della Pubblica Amministrazione e/o di Funzionari che agiscono per conto della Pubblica Amministrazione.

Al fine di prevenire tali comportamenti, si precisa che ai Dipendenti dell'azienda, agli Amministratori, Consulenti, Collaboratori esterni e Partner dell'azienda, è vietato:

- offrire denaro o doni a dirigenti, funzionari o dipendenti della Pubblica Amministrazione o a loro parenti, salvo che non si tratti di doni o utilità d'uso di modico valore;
- offrire qualsiasi oggetto, servizio, prestazione o favore di valore per ottenere un trattamento più favorevole in relazione a qualsiasi rapporto intrattenuto con la Pubblica Amministrazione;
- cercare di influenzare impropriamente i Funzionari o i Collaboratori della Pubblica Amministrazione, quando è in corso una qualsiasi trattativa, richiesta o rapporto con la Pubblica Amministrazione stessa;
- esaminare o proporre opportunità di impiego e/o commerciale che possano avvantaggiare dipendenti della Pubblica Amministrazione a titolo personale;
- sollecitare e/o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti.

Qualsiasi violazione (effettiva o potenziale) delle norme di condotta incluse nel presente paragrafo, commessa dai dipendenti della SO.GE.R.T. S.p.A. o da qualsiasi soggetto destinatario del presente Codice Etico, deve essere segnalata tempestivamente all'Organismo di Vigilanza.

2.6 Rapporti con i mass media

Le comunicazioni della Società verso l'ambiente esterno devono essere veritiere, chiare, trasparenti e non ambigue o strumentali.

Le notizie che SO.GE.R.T. S.p.A. fornisce ai *mass media* dovranno essere accurate ed omogenee e dovranno essere divulgate solo dalle persone a ciò delegate.

I dipendenti della SO.GE.R.T. S.p.A. non possono fornire informazioni ai rappresentanti dei *mass media* senza l'autorizzazione degli organi competenti.

I rapporti con la stampa devono essere tenuti solo da persone autorizzate a farlo nell'interesse dell'azienda.

Le informazioni dovranno essere coerenti con le politiche dell'azienda.

2.7 Partecipazione a procedure di gara indette dalla Pubblica Amministrazione

La SO.GE.R.T. S.p.A. si impegna a partecipare alle procedure di gara indette dalla Pubblica Amministrazione in modo corretto, nel rispetto della legge, delle norme del presente Codice Etico e delle procedure interne.

E' pertanto vietato ai dipendenti, agli Organi ed ai Collaboratori dell'azienda:

- promettere/dare ad un Pubblico Ufficiale, per lui o per un terzo, una retribuzione non dovuta in denaro od altra attività in cambio di un atto del suo ufficio necessario per l'avanzamento dell'azienda nella procedura di gara;
- promettere/dare ad un Pubblico Ufficiale, per lui o per un terzo, una somma di denaro od un'altra utilità al fine di fargli omettere/ritardare un atto del suo ufficio o per compiere un atto contrario ai doveri d'ufficio al fine di favorire l'avanzamento dell'azienda nella procedura di gara;
- indurre con artifici o raggiri, lo Stato o un qualsiasi Ente Pubblico in errore al fine di favorire l'avanzamento della Società nella procedura di gara;

2.8 Richiesta di fondi pubblici e loro gestione

In relazione alle richieste di Fondi Pubblici ed al loro utilizzo, SO.GE.R.T. S.p.A. si impegna a procedere nell'iter per l'ottenimento dei fondi e nel loro utilizzo in modo corretto, nel rispetto della legge, delle norme del presente Codice Etico e delle procedure interne.

E' pertanto vietato ai dipendenti, agli Organi ed ai Collaboratori dell'Azienda:

- impiegare i fondi ricevuti per favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse con finalità diverse da quelle per cui sono stati ottenuti;
- utilizzare/presentare dichiarazioni o documenti falsi attestanti cose non vere o omettere informazioni dovute al fine di conseguire indebitamente i fondi;

- promettere/dare ad un Pubblico Ufficiale, per lui o per un terzo, una retribuzione non dovuta in denaro od altra attività in cambio di un atto del suo ufficio necessario per l'ottenimento di fondi a favore dell'azienda;
- promettere/dare ad un Pubblico Ufficiale, per lui o per un terzo, una somma di denaro od un'altra utilità al fine di fargli omettere/ritardare un atto del suo ufficio o per compiere un atto contrario ai doveri d'ufficio al fine di favorire l'ottenimento di fondi a favore dell'azienda;
- indurre con artifici o raggiri, lo Stato o un qualsiasi Ente Pubblico in errore al fine di far ottenere all'azienda i Fondi;
- alterare in qualsiasi modo il funzionamento di un sistema informatico/telematico o intervenire su dati/informazioni/programmi per ottenere i fondi o aumentare l'importo di Fondi già ottenuti.

2.9 Partecipazione a procedimenti giudiziari

SO.GE.R.T. S.p.A. si impegna ad attivarsi nel procedimento giudiziario in modo corretto, nel rispetto della legge, delle norme del presente Codice Etico e delle procedure interne.

SO.GE.R.T. S.p.A., favorisce il dialogo e la collaborazione con contribuenti e fornitori e privilegia la risoluzione in via non giudiziale dei possibili contrasti promuovendo procedure conciliative per prevenire le controversie giudiziali tra l'azienda e il contribuente.

All'interno dei procedimenti giudiziari in cui l'azienda sia parte, è vietato ai Dipendenti, agli Organi dell'azienda e ai Collaboratori dell'azienda:

- promettere/dare ad un Pubblico Ufficiale, per lui o per un terzo, una retribuzione non dovuta in denaro od altra attività in cambio di un atto del suo ufficio al fine di ottenere un vantaggio per l'azienda;
- promettere/dare ad un Pubblico Ufficiale, per lui o per un terzo, una somma di denaro od un'altra utilità al fine di fargli omettere/ritardare un atto del suo ufficio o per compiere un atto contrario ai doveri d'ufficio al fine di ottenere un vantaggio dell'azienda nel procedimento giudiziario;

- indurre con artifici o raggiri, lo Stato o un qualsiasi Ente Pubblico in errore al fine di ottenere un vantaggio per l'azienda nel procedimento giudiziario;
- alterare in qualsiasi modo il funzionamento di un sistema informatico/telematico o intervenire su dati/informazioni/programmi al fine di ottenere un vantaggio per l'azienda nel procedimento giudiziario.

2.10 Relazioni con partiti politici, organizzazioni sindacali e associazioni portatrici di interessi

Nei rapporti con partiti politici, organizzazioni politiche e sindacali e associazioni rappresentative di interessi collettivi o di categoria, l'Azienda si attiene scrupolosamente al Codice Etico e tiene conto dei rispettivi ruoli nell'ambito dell'agire sociale.

I rapporti in questione sono intrattenuti esclusivamente dagli Esponenti Aziendali o dai Dipendenti competenti secondo le norme interne dell'Azienda o espressamente e debitamente autorizzati, con il conferimento di adeguati poteri.

E' sempre tassativamente vietato promettere o corrispondere, a qualsiasi titolo, anche indirettamente, o sotto forme simulate, denaro o altre utilità a persone che fanno parte di partiti politici, organizzazioni politiche e sindacali e associazioni rappresentative di interessi collettivi o di categoria o a persone a queste collegate in virtù di rapporti familiari, personali o d'affari.

Chiunque venga a conoscenza di richieste di denaro o altra utilità provenienti da persone facenti parte di partiti politici, organizzazioni politiche e sindacali e associazioni rappresentative di interessi collettivi o di categoria, o comunque di promesse o dazioni di denaro o altra utilità effettuate da parte di esponenti aziendali in favore dei soggetti predetti, è tenuto ad informare tempestivamente il responsabile della funzione e/o l'Organismo di Vigilanza.

Solo nel perseguimento di scopi istituzionali, culturali o di solidarietà sociale, l'azienda può promuovere o partecipare, anche con contribuzioni di denaro o offerta di servizi, a iniziative coerenti alle finalità predette. In base alle norme interne dell'azienda la partecipazione all'iniziativa deve essere adeguatamente motivata, anche riguardo alla congruità dell'impegno economico ed alla qualità dell'iniziativa e dei partecipanti.

2.11 Rapporti con le Autorità di Vigilanza e Controllo

I rapporti dell'azienda con le Autorità di vigilanza e controllo, siano esse nazionali, o sovranazionali, sono ispirati ai principi di legalità, trasparenza e leale collaborazione.

SO.GE.R.T. S.p.A. dà piena e scrupolosa osservanza alle norme *antitrust* ed alle *Authorities* regolatrici del mercato.

L'azienda, ove richiesto dalle normative vigenti, mantiene puntuali flussi informativi con le Autorità, assicurando la completezza e la veridicità delle notizie fornite.

L'azienda adempie gli obblighi di legge in materia di comunicazioni nei confronti delle competenti Autorità garantendo la completezza e l'integrità delle notizie, l'oggettività delle valutazioni e assicurando la tempestività nell'inoltro.

2.12 Rapporti con il Collegio Sindacale, le Società di revisione e altre strutture.

Nei rapporti con il Collegio Sindacale e con la Società di revisione, ove presente, ciascuna struttura o funzione dell'azienda, nonché ciascun Destinatario si attiene, tra l'altro, alle disposizioni del Codice, nel rispetto dei rispettivi ruoli istituzionali.

Le richieste di adempimenti e di documentazione devono essere evase tempestivamente, con chiara assunzione della responsabilità circa la veridicità, completezza e accuratezza delle informazioni fornite. I dati ed i documenti richiesti sono resi disponibili in modo puntuale ed esauriente. Le informazioni così fornite devono essere accurate, complete, fedeli e veritiere evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse.

2.13 Informazioni riservate e protezione dei dati personali

Per informazioni riservate si intendono i dati e le conoscenze non accessibili al pubblico, in qualsiasi modo elaborate o registrate, attinenti all'organizzazione dell'azienda, ai beni aziendali, alle operazioni commerciali e finanziarie progettate o avviate dall'azienda, ai procedimenti giudiziali ed amministrativi, ai rapporti con i contribuenti e con i fornitori della SO.GE.R.T.

S.p.A. e le altre controparti istituzionali.

In ogni comunicazione con l'esterno le informazioni riguardanti l'azienda e le sue attività devono essere veritiere, chiare, verificabili.

Nessuna informazione riservata relativa all'azienda, acquisita o elaborata nello svolgimento o in occasione delle diverse attività, può essere utilizzata, comunicata a terzi o diffusa, se non nei limiti delle esigenze imposte da una corretta attività lavorativa e, in ogni caso, mai per fini diversi da quelli istituzionali.

Le persone che, secondo i regolamenti interni, sono a conoscenza di informazioni riservate, o ne vengono occasionalmente a conoscenza sono tenute a rispettare i vincoli di riservatezza stabiliti dall'azienda.

Il dipendente, al fine di tutelare la riservatezza delle informazioni comunicate dalle imprese che entrano in contatto con l'azienda si astiene dal diffondere e dall'utilizzare, a scopo personale, le informazioni di cui dispone per ragioni d'ufficio, fermo restando il rispetto delle norme e dei regolamenti posti a tutela del diritto di informazione e di accesso.

Ciascun dipendente deve conoscere e attuare quanto previsto dalle politiche aziendali in tema di sicurezza delle informazioni per garantirne l'integrità, la riservatezza e la disponibilità.

Fermo restando il rispetto della normativa vigente in materia di tutela e trattamento dei dati personali, i Destinatari del Codice assicurano l'utilizzo di informazioni riservate solo per scopi connessi all'esercizio della propria attività, impegnandosi a proteggere le informazioni generate o acquisite e ad evitarne ogni uso improprio o non autorizzato.

2.14 Doni, benefici o altre utilità

E' vietato a tutti i Destinatari promettere od offrire a terzi, nonché accettare la promessa di o ricevere da terzi, direttamente o indirettamente, anche in forme simulate, doni, benefici o altre utilità (es. economici, favori, raccomandazioni).

Il divieto che precede ammette deroghe per beni o servizi di modico valore la cui offerta rientri nelle consuetudini, sempre che essi non siano stati sollecitati dal Destinatario e non siano tali da poter suscitare l'impressione che la loro offerta comporti indebiti vantaggi per chicchessia.

In ogni caso il destinatario è tenuto a comunicare all'Organismo di Vigilanza la deroga.

Analogamente il Destinatario che riceve beni, servizi o altre utilità in modo difforme da quanto precede deve informare immediatamente il responsabile della funzione e l'Organismo di Vigilanza.

2.15 Utilizzo di attrezzature, dispositivi e strutture aziendali

Il patrimonio aziendale della SO.GE.R.T. S.p.A. è costituito dai beni fisici materiali, quali ad esempio attrezzature, automezzi, impianti, immobili, computer, stampanti, software e infrastrutture e beni immateriali quali ad esempio, informazioni riservate, know-how, conoscenze tecniche, sviluppate e diffuse dai dipendenti della Società.

Tutti devono sentirsi responsabili dei beni della SO.GE.R.T. S.p.A. e del loro corretto utilizzo.

L'utilizzo di questi beni da parte dei destinatari, deve essere funzionale esclusivamente allo svolgimento delle attività aziendali o agli scopi autorizzati dalle funzioni aziendali interessate.

Eventuali deroghe sono consentite solo se debitamente autorizzate.

E' fatto assoluto divieto di utilizzare in modo improprio o danneggiare i beni e le risorse dell'azienda o di consentire ad altri di farlo.

L'impiego dei beni aziendali deve essere sempre conforme alle leggi, al Codice e alle norme interne e deve essere effettuato secondo i principi di funzionalità ed efficienza.

Le registrazioni o riproduzioni audiovisive, elettroniche o fotografiche di documenti aziendali sono consentite solo per le esigenze direttamente connesse allo svolgimento della mansione o funzione attribuita, e sempre che non si pongano in conflitto con gli interessi dell'azienda.

In ogni caso, i Destinatari non possono utilizzare le risorse, i programmi e le apparecchiature informatiche e di rete per finalità estranee a quelle dell'azienda o contrarie alla normativa ed al presente Codice e sempre nel rispetto della regolamentazione aziendale sull'uso degli strumenti informatici, della c.d. e-mail, della rete *internet* messa a disposizione dall'azienda e delle apparecchiature di telefonia fissa e mobile in dotazione.

2.16 Registrazioni contabili

Le scritture contabili devono essere redatte secondo i principi di trasparenza, veridicità, completezza, chiarezza, affidabilità, ricostruibilità e devono consentire la redazione di un quadro

attendibile e fedele della situazione economico-patrimoniale dell'azienda.

Deve essere assicurata la possibilità di rintracciare agevolmente, per ciascun documento contabile, la documentazione che lo supporta, al fine di consentire analisi e verifiche.

La documentazione deve altresì consentire di ricostruire i soggetti che sono intervenuti nella preparazione dell'operazione, nella sua decisione o attuazione e nel controllo, nonché le modalità seguite e i criteri adottati nelle valutazioni.

Devono essere attuate adeguate ed opportune modalità di conservazione della documentazione contabile, al fine di garantire la autenticità e la veridicità di ciascun documento.

Le rappresentazioni in bilancio di fatti di gestione a supporto di valutazioni estimative, dovranno consentire di scindere il contenuto rappresentativo da quello valutativo, indicando in modo chiaro e preciso i criteri assunti a base della valutazione.

3. Risorse umane

SO.GE.R.T. S.p.A. riconosce la centralità delle risorse umane, quale principale fattore di successo di ogni impresa, in un quadro di lealtà e fiducia reciproche tra datore e prestatori di lavoro.

Il rapporto di lavoro si svolge nel rispetto della normativa contrattuale collettiva del settore e della normativa previdenziale, fiscale ed assicurativa.

La selezione, la retribuzione, la formazione e la progressione delle carriere del personale devono basarsi su criteri predeterminati ed oggettivi, ispirati a correttezza, imparzialità e merito.

Le assunzioni avvengono con regolare contratto di lavoro nel rispetto di tutte le norme legali e contrattuali, favorendo l'inserimento del lavoratore nell'ambiente di lavoro. L'Azienda favorisce la crescita professionale e personale dei Dipendenti e a tal fine ha cura di coinvolgerli nella condivisione degli obiettivi e nell'assunzione di responsabilità coerenti con i ruoli ricoperti e le capacità riscontrate. Ciascun Dipendente ha diritto a svolgere mansioni coerenti con quelle per le quali è stato assunto o che gli sono state assegnate in ragione dei suoi meriti e della sua crescita professionale.

Le decisioni relative alla selezione del personale e tutte le decisioni relative ai rapporti di lavoro devono essere motivate.

È vietato anche il solo prospettare (i) incrementi nella remunerazione, (ii) altri vantaggi o (iii) progressione di carriera, quale contropartita di attività difforni dalle leggi, dal Codice e dalle norme e regole interne.

3.1 Conflitto di interessi e attività lavorativa esterna da parte dei dipendenti

Il dipendente della SO.GE.R.T. S.p.A. deve astenersi dal partecipare a qualsiasi attività che possa ingenerare conflitto di interessi.

Per conflitto di interessi si intende che i dipendenti debbano evitare tutte le situazioni ed attività in cui si possa manifestare un conflitto di interessi tra le attività economiche personali e le mansioni che ricoprono all'interno della struttura di appartenenza.

Il personale della SO.GE.R.T. S.p.A. nello svolgimento delle proprie attività non può:

- svolgere attività lavorative a favore della concorrenza;
- prestare, senza il consenso della Società, la propria attività professionale in qualità di dipendente, consulente, Amministratore o membro del Collegio Sindacale, a favore di organizzazioni concorrenti della SO.GE.R.T. S.p.A.;
- utilizzare sul lavoro o nel tempo libero beni aziendali o fornire servizi che SO.GE.R.T. S.p.A. offre ai propri contribuenti;
- rappresentare, agire e lavorare per conto di un fornitore o un contribuente della SO.GE.R.T. S.p.A.

È proibito accettare e/o ricevere denaro o altri favori per consigli o servizi resi, in relazione alla normale attività.

4. Ambiente

La politica ambientale della SO.GE.R.T. S.p.A., nasce dalla consapevolezza che l'ambiente e lo sviluppo sostenibile rappresentano un vantaggio competitivo in un mercato sempre più attento alla qualità dei prodotti e dei servizi.

Al fine di un perfezionamento continuo delle sue prestazioni relativamente agli impatti ambientali della sua attività, SO.GE.R.T. S.p.A., si impegna a:

- adottare sistemi di gestione ambientale e di qualità certificati e operare per la prevenzione dei rischi ambientali;

- definire specifici obiettivi e programmi di miglioramento, volti alla minimizzazione degli impatti ambientali significativi;
- diffondere sul territorio la cultura del rispetto dell'ambiente anche attraverso iniziative dedicate, nonché specifici servizi al contribuente;
- fornire alle istituzioni tutte le informazioni necessarie a comprendere gli eventuali rischi ambientali legati all'attività dell'impresa;
- promuovere attività di sensibilizzazione e di formazione ambientale al proprio interno e promuovere la diffusione di tecnologie eco-efficienti;
- rendere conto dell'impatto ambientale delle proprie attività attraverso l'individuazione di indicatori chiave di performance.

In quest'ottica, ogni dipendente e collaboratore è personalmente responsabile, verso i colleghi e l'azienda, per il mantenimento della qualità di tale ambiente. Agli stessi si richiede, pertanto, di non contribuire e, ove possibile, di prevenire o limitare eventuali situazioni che possano deteriorare la suddetta qualità

5. Salute e Sicurezza sul lavoro

La tutela della salute e sicurezza dei lavoratori negli ambienti di lavoro è per la SO.GE.R.T. S.p.A. un principio di grande significato e spessore culturale.

A tal fine, SO.GE.R.T. S.p.A. si pone l'obiettivo di "lavorare in sicurezza", ovvero di garantire il rispetto delle norme di prevenzione e l'adozione di comportamenti sicuri a vantaggio della tutela delle persone e dell'ambiente di lavoro.

L'azienda si impegna, quindi, a garantire l'integrità fisica e morale dei suoi collaboratori e dipendenti, condizioni di lavoro rispettose della dignità individuale e un ambiente di lavoro sicuro, sano e produttivo anche tramite la diffusione di una cultura della sicurezza e della consapevolezza dei rischi, e l'incentivazione di comportamenti responsabili da parte di tutti.

SO.GE.R.T. S.p.A. svolge la propria attività a condizioni tecniche, organizzative ed economiche tali da consentire che siano assicurati una adeguata prevenzione infortunistica ed un ambiente di lavoro salubre e sicuro.

L'azienda si impegna a diffondere e consolidare tra tutti i propri collaboratori e dipendenti una cultura della sicurezza, sviluppando la consapevolezza dei rischi e promuovendo comportamenti sicuri e responsabili da parte dei singoli.

L'azienda, pertanto, si impegna a porre in essere attività sicure al fine di proteggere la salute dei propri dipendenti e delle comunità che circondano i propri impianti e ad uniformare le proprie strategie operative al rispetto delle leggi vigenti in materia di sicurezza, salute e ambiente.

L'azienda inoltre riesamina periodicamente le prestazioni e l'efficienza dei propri sistemi, per raggiungere gli obiettivi prefissati in materia di sicurezza, salute e ambiente.

L'azienda ispira la propria attività ai seguenti principi e criteri in materia di salute e sicurezza sul lavoro:

- a) evitare i rischi;
- b) valutare i rischi che non possono essere evitati;
- c) combattere i rischi alla fonte;
- d) adeguare il lavoro all'uomo, in particolare per quanto concerne la concezione dei posti di lavoro e la scelta delle attrezzature di lavoro e dei metodi di lavoro, in particolare per attenuare il lavoro monotono e il lavoro rispettivo e per ridurre gli effetti di questi lavori sulla salute;
- e) tener conto del grado di evoluzione della tecnica;
- f) sostituire ciò che è pericoloso con ciò che non è pericoloso o è meno pericoloso;
- g) programmare la prevenzione, mirando ad un complesso coerente che integri nella medesima tecnica, l'organizzazione del lavoro, le condizioni di lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro;
- h) dare la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale;
- i) impartire adeguate istruzioni ai lavoratori.

L'azienda si impegna, nello specifico, ad attenersi ai principi e criteri fondamentali esplicitati nel Sistema di Gestione Sicurezza sul Lavoro (SGSL) - Politica della Sicurezza, nell'espletamento di ogni attività, comprese le attività di prevenzione dei rischi professionali, d'informazione e formazione, l'approntamento di un'organizzazione dei mezzi necessari a garantire la salute e sicurezza sul lavoro.

SO.GE.R.T. S.p.A., sia ai livelli apicali che a quelli operativi, in relazione a ciascuna funzione, deve attenersi a questi principi ogni qual volta siano prese delle decisioni o fatte delle scelte e, in seguito, quando le stesse siano attuate.

I lavoratori, analogamente, dovranno garantire il rispetto delle seguenti regole:

- adottare comportamenti sicuri durante il lavoro, ovvero operare nel rispetto dei regolamenti aziendali, delle procedure, delle istruzioni, delle norme di prevenzione in generale e del presente Codice etico;
- evitare comportamenti pericolosi per sé e per gli altri;
- rispettare gli ordini indicati dai superiori gerarchici o dalla Direzione;
- comunicare immediatamente ai superiori ogni anomalia, criticità o altra situazione di pericolo di cui si venga a conoscenza durante il lavoro;
- comunicare immediatamente al proprio preposto (che avvertirà, tramite la gerarchia aziendale, l'Organismo di Vigilanza) all'esclusivo fine di tutelare la sicurezza propria e dei colleghi di lavoro, il mancato rispetto altrui delle procedure di sicurezza nell'espletamento delle mansioni;
- rispettare i compiti e le attribuzioni assegnate;
- prestare la massima collaborazione alle attività o alle indicazioni del Servizio di Prevenzione e Protezione;
- coinvolgere il RSGSL in ordine alle rilevate anomalie o criticità e collaborare con il responsabile per l'adeguamento o il miglioramento delle misure;
- partecipare con attenzione alle attività formative organizzate;
- collaborare, con comportamenti responsabili e nel rispetto delle regole aziendali, nel caso di allarme per una situazione di emergenza;
- sottoporsi alla sorveglianza sanitaria prevista;
- maturare la piena consapevolezza in merito all'attuazione del modello organizzativo e di gestione adottato, collaborando con le figure responsabili al raggiungimento degli obiettivi di prevenzione.

I collaboratori/fornitori e terzi dovranno anch'essi garantire il rispetto delle seguenti regole:

- adottare comportamenti sicuri durante le loro attività, ovvero operare nel rispetto dei regolamenti aziendali, delle istruzioni ricevute, delle norme di prevenzione in generale e del presente Codice Etico;
- rispettare le condizioni contrattuali che regolamentano il rapporto tra le parti;

6. Remunerazione

La determinazione e la gestione del sistema delle remunerazioni è affidato al Consiglio di Amministrazione.

Fermo restando il rispetto di norme imperative, delle norme e degli accordi sindacali, il sistema delle remunerazioni, a qualsiasi livello, sia nella parte in denaro che in quella costituita da *benefit*, deve essere ispirato a criteri predeterminati e conoscibili.

Tali criteri attuano il principio per cui la remunerazione deve essere determinata unicamente sulla base di valutazioni oggettive attinenti alla formazione scolastica, alla professionalità specifica, all'esperienza acquisita, al merito dimostrato ed al raggiungimento degli obiettivi assegnati.

7. Attività collaterali

Lo svolgimento di attività lavorative, anche saltuarie o gratuite, al di fuori dell'azienda, è consentito ai Destinatari nei limiti in cui non ostacoli l'adempimento dei loro doveri nei confronti dell'azienda, fermo restando che tali attività non devono pregiudicare gli interessi dell'azienda o la sua reputazione.

Per i lavoratori subordinati vigono in particolare le disposizioni al riguardo contenute nel contratto collettivo nazionale di settore con i divieti di attività ivi contenuti.

8. Prevenzione

Nel rispetto della normativa vigente e nell'ottica della pianificazione e della gestione delle attività aziendali tese all'efficienza, alla correttezza, alla trasparenza ed alla qualità, SO.GE.R.T. S.p.A. adotta misure organizzative e di gestione idonee a prevenire comportamenti illeciti o comunque contrari alle regole di questo Codice da parte di qualunque soggetto che agisca per suo conto.

In ragione dell'articolazione delle attività e della complessità organizzativa, SO.GE.R.T. S.p.A. adotta un sistema di deleghe di poteri e funzioni, prevedendo in termini espliciti e specifici l'attribuzione degli incarichi a persone dotate di idonea capacità e competenza.

In relazione all'estensione dei poteri delegati, SO.GE.R.T. S.p.A. adotta ed attua modelli di organizzazione e gestione che prevedono misure idonee a garantire lo svolgimento delle attività nel rispetto della legge e delle regole di comportamento di questo Codice, ed a scoprire ed eliminare tempestivamente le situazioni di rischio.

9. Controlli

SO.GE.R.T. S.p.A., adotta specifiche modalità di controllo della conformità dei comportamenti, di chiunque agisca per suo conto o nel suo ambito, alle previsioni della normativa vigente ed alle regole di comportamento di questo Codice.

Ciascun Destinatario del presente Codice, nell'ambito delle proprie funzioni e dei compiti assegnati, deve contribuire attivamente al corretto funzionamento del sistema dei controlli interni.

10. Sanzioni

L'osservanza da parte dei dipendenti dell'azienda delle norme del Codice Etico deve considerarsi parte essenziale delle obbligazioni contrattuali ai sensi dell'art. 2104 c.c.

La violazione delle norme del Codice Etico da parte del personale dipendente potrà costituire inadempimento alle obbligazioni primarie del rapporto di lavoro o illecito disciplinare, con ogni conseguenza di legge.

Fatta salva la possibilità per l'azienda di chiedere il risarcimento dei danni che alla stessa possano derivare da comportamenti in violazione del Codice Etico adottato, l'inosservanza delle norme in esso contenute, comporta l'applicazione ai Destinatari di una sanzione proporzionata, efficace e dissuasiva.

Sono prese in considerazione sia violazioni consumate che tentate, garantendo il sistema delle sanzioni una adeguata graduazione della risposta sanzionatoria. Sono altresì sanzionate anche le condotte consapevolmente volta all'elusione delle norme prima richiamate.

L'applicazione delle sanzioni nei confronti dei Dipendenti avviene nel rispetto delle disposizioni di legge e delle previsioni contenute negli accordi – anche individuali – e nei contratti collettivi

di lavoro, in particolare con riferimento agli artt. 7 e segg. della Legge 20 maggio 1970, n. 300 e delle disposizioni contenute nei C.C.N.L. applicabili.

Per i Destinatari diversi dai Dipendenti, la sanzione delle violazioni del Codice deve essere prevista nello strumento contrattuale o nella delibera degli Organi dell'azienda che regola il rapporto. L'Organo Amministrativo adotta gli opportuni provvedimenti nei confronti dei suoi membri che abbiano commesso violazioni del Codice.

In caso di violazioni commesse dagli Amministratori, l'Organismo di Vigilanza informerà il Collegio Sindacale, il quale provvederà ad assumere le opportune iniziative previste dalla vigente normativa.

11. Segnalazioni.

Ogni Destinatario ha l'obbligo di segnalare al Presidente dell'Organismo di Vigilanza immediatamente qualsiasi violazione del Codice Etico o del Modello di Organizzazione e Gestione.

Le segnalazioni all'Organismo di Vigilanza possono essere inviate tramite una apposita casella di posta elettronica.

Con riferimento alle segnalazioni ricevute, l'Organismo di Vigilanza potrà avvalersi delle competenti funzioni aziendali – ed in particolare delle strutture deputate al controllo interno – per gli accertamenti del caso e potrà proporre l'adozione dei provvedimenti necessari.

Tutte le segnalazioni pervenute all'Organismo di Vigilanza vengono gestite in modo confidenziale: il Modello di Organizzazione e Gestione o il regolamento dell'Organismo di Vigilanza impegna i membri di quest'ultimo al mantenimento della riservatezza sulle segnalazioni ricevute ed è sempre garantito l'anonimato del soggetto che le effettua.

I soggetti che segnalano in buona fede devono essere garantiti contro qualsiasi forma di ritorsione, discriminazione, penalizzazione e in ogni caso sarà assicurata la riservatezza dell'identità di coloro che segnalano, fatti salvi gli obblighi di legge e la tutela dei diritti dell'azienda o delle persone accusate erroneamente o in malafede.

A seguito dell'entrata in vigore della L. 179/2017 recante “Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato”, la Società tutela i soggetti apicali e coloro che sono da questi diretti o controllati, che segnaleranno azioni circostanziate di condotte illecite rilevanti in materia di

responsabilità amministrativa da reato degli enti, fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del Modello Organizzativo.

Verrà, inoltre, garantita la riservatezza dell'identità dei segnalanti e gli stessi saranno tutelati da eventuali atti di ritorsione o di discriminazione per l'avvenuta segnalazione.



SO.GE.R.T. S.P.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX DECRETO

LEGISLATIVO 8 GIUGNO 2001 N. 231

CON SPECIFICHE PREVISIONI EX LEGGE 190/2012

▪

▪

aggiornato al 29 dicembre 2023

INDICE

PARTE GENERALE

1.	Il Decreto Legislativo 8 giugno 2001 n. 231.....	5
1.1	Il Modello di responsabilità da reato della Società o Ente.....	5
1.1.1	Reati per i quali è prevista la responsabilità da reato della Società o Ente.....	6
1.1.2	Il D.lgs. 231/2001 e il fenomeno corruttivo ex L. 190/2012.....	12
1.1.3	Specifiche prescrizioni su antiriciclaggio e ricettazione.....	17
1.1.4	I reati Ambientali.....	20
1.1.5	Le sanzioni applicabili.....	27
1.1.6	Responsabilità della Società e vicende modificative.....	29
1.1.7	L'adozione del Modello Organizzativo, quale circostanza esimente della responsabilità amministrativa da reato.....	31
1.1.8	La costruzione del Modello di Organizzazione, Gestione e Controllo.....	33
1.2	La tutela del Whistleblower.....	37
1.2.1	Specifiche prescrizioni in materia di Whistleblowing.....	39
2.	Il Modello di Organizzazione, Gestione e Controllo predisposto dalla SO.GE.R.T. S.p.A.....	43
2.1	Finalità del Modello.....	46
2.2	Costruzione del Modello.....	49
2.2.1	Struttura del Modello.....	50
2.2.2	Adozione del Modello nell'ambito della SO.GE.R.T. S.p.A.....	51
2.2.3	Attuazione del Modello all'interno della SO.GE.R.T. S.p.A.....	52
2.2.4	Destinatari del Modello.....	52
2.2.5	Il Codice Etico.....	53
2.2.6	Organismo di Vigilanza.....	54
2.2.7	Comunicazione e Formazione.....	57
2.2.7.1	Informativa ai soggetti terzi, esterni alla compagine della Società.....	57
2.2.7.2	I flussi informativi che coinvolgono l'Organismo di Vigilanza.....	59
2.2.8	Sistema disciplinare.....	62
3.	Il Modello di <i>Governance</i> ed il Sistema Organizzativo.....	64
3.1	Il Modello di <i>Governance</i> della SO.GE.R.T. S.p.A.....	64
3.2	Struttura Organizzativa della SO.GE.R.T. S.p.A.....	66
3.3	Descrizione delle deleghe e individuazione dei soggetti 'apicali' e 'subalterni'.....	70
4.	Identificazione delle aree della Società a rischio reato (<i>Risk Assessment</i>) e verifica dei sistemi di controllo esistenti (<i>Gap Analysis</i>).....	71
a.	<i>Risk Assessment</i> e <i>Gap Analysis</i>	71
5.	Comunicazione e Formazione.....	77
5.1	Diffusione del Modello.....	77
5.2	Formazione e addestramento sul Modello e sui Protocolli etico-organizzativi.....	78

PARTE SPECIALE

Protocolli etico-organizzativi

PRO.1 – Gestione dei rapporti con la Pubblica Amministrazione

PRO.2 – Salute e Sicurezza sul lavoro

PRO.3 – Prevenzione reati informatici e trattamento illecito dei dati

PRO. 4 – Prevenzione reati tributari

ALLEGATI

1. Matrice Aree a rischio
2. Regolamento Organismo di Vigilanza
3. Codice Etico
4. Sistema Disciplinare

PARTE GENERALE

1. Il Decreto Legislativo 8 giugno 2001 n. 231

1.1 Il Modello di responsabilità da reato della Società o Ente

Con il Decreto Legislativo n. 231 dell'8 giugno 2001, recante la *“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”*, è stata introdotta nell'ordinamento vigente la c.d. *responsabilità amministrativa da reato* degli Enti e, più in generale, degli altri soggetti, (se pubblici, solo economici) forniti o meno di personalità giuridica, che esso descrive all'art. 1.

Con quest'intervento normativo, l'ordinamento interno si adegua alle numerose Convenzioni internazionali sottoscritte da tempo dall'Italia, in particolare le Convenzioni di Bruxelles del 26 luglio 1995 e del 26 maggio 1997, rispettivamente, sulla tutela degli interessi finanziari della Comunità Europea e sulla lotta alla corruzione di funzionari pubblici della Comunità Europea e degli Stati membri, e alla Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

In riferimento a questa importante cornice normativa di matrice sovranazionale, il Decreto ha imposto agli Enti (di cui al citato art.1) l'adozione di protocolli e procedure di auto-controllo, rispetto alla prevenzione delle ipotesi di reato riconsiderate dalla stessa normativa quali fonti della responsabilità da reato dell'Ente.

Qualora, cioè, esse accadano e la loro realizzazione sia imputabile alla mancata diligente ed efficace attuazione di questo corpo auto normativo penal-preventivo di cui l'Ente deve essersi nel frattempo dotato, può derivarne l'accertamento della responsabilità da parte dello stesso giudice competente a conoscere e punire gli autori individuali del reato.

Come è immediatamente evidente, per il novero dei reati selezionati da Decreto Legislativo n. 231 del 2001, si realizza un notevole ampliamento delle figure responsabili, essendosi affiancata alla tradizionale punibilità delle persone fisiche, autori materiali dell'illecito, anche quella dell'Ente che abbia tratto vantaggio dal reato, o nel cui interesse questo sia stato commesso (art. 5), anche per i reati ad esso riferibili commessi all'estero, purché per gli stessi non proceda lo Stato nel cui luogo è stato commesso il reato (art. 4).

1.1.1 Reati per i quali è prevista la responsabilità da reato della Società o Ente

La responsabilità da reato dell'Ente è circoscritta dal D. Lgs. n. 231/2001 attraverso due distinte cornici normative; la prima, di matrice soggettiva, è relativa all'individuazione dei soggetti di cui, ai sensi del Decreto, rilevano le condotte costituenti reato, in riferimento alle funzioni dell'Ente da essi svolte. La seconda di carattere oggettivo, evidenzia come la responsabilità della Società sorga in dipendenza della realizzazione di alcuni reati, da parte dei soggetti individuati nel Decreto, nell'interesse o a vantaggio della Società medesima. Occorre chiarire, quindi, che la responsabilità amministrativa della Società non è configurabile in conseguenza della commissione di tutti i reati previsti nell'ordinamento, bensì solo con riferimento ad alcune fattispecie criminosi, espressamente indicate dal Legislatore.

La Società, pertanto, è responsabile per i reati commessi nel suo interesse o a suo vantaggio da:

- **persone fisiche che rivestono posizioni cc.dd. “apicali”** (rappresentanza, amministrazione o direzione della Società o di altra unità organizzativa o persone che ne esercitino, di fatto, la gestione e il controllo, ex art. 5 d.lgs. n.231/2001).
- **persone fisiche cc.dd. “sottoposte”** alla direzione o vigilanza dei soggetti sopraindicati (ex art. 5 d.lgs. n.231/2001), ovvero i dipendenti della Società.

In riferimento all’ambito oggettivo del reato, la responsabilità della Società sussiste solo rispetto alle figure criminose per le quali essa è espressamente prevista, secondo la clausola di tassatività dettata dall’art. 2 d.lgs. n. 231/01.

Il novero dei reati – presupposto della responsabilità della Società – è quello individuato dalla cd. *parte speciale* del Decreto n. 231/2001, di cui agli artt. 24, 24*bis*, 24*ter*, 25, 25*bis*, 25*bis*.1, 25*ter*, 25*quater*, 25*quater*.1, 25*quinqies*, 25*sexies*, 25*septies*, 25*octies*, 25*octies*.1, 25*novies*, 25*decies*, 25*undecies*, 25*duodecies*, 25*terdecies*, 25*quaterdecies*, 25*quindecies*, 25*sexdecies*, 25*septiesdecies*, 25*duodevicies*.

L’ Ente risponde anche nel caso di delitti commessi in forma tentata.

In particolare, i cd. reati presupposto o reati di collegamento ai fini della responsabilità della Società previsti dai predetti articoli sono i seguenti:

Norma di riferimento	Reato presupposto
Reati contro la Pubblica Amministrazione (artt. 24 e 25)	Art. 316 bis c.p. - (Malversazione a danno dello Stato)
	Art. 316 ter c.p. - (Indebita percezione di erogazioni a danno dello Stato)
	Art. 640 c.p. - (Truffa)
	Art. 640 bis c.p. - (Truffa aggravata per il conseguimento di erogazioni pubbliche)
	Art. 640 ter c.p. - (Frode informatica)
	Art. 317 c.p. - (Concussione)
	Art. 318 c.p. - (Corruzione per l'esercizio della funzione)
	Art. 319 c.p. - (Corruzione per un atto contrario ai doveri d'ufficio)
	Art. 319 bis c.p. - (Circostanze aggravanti)
	Art. 319 ter c.p. - (Corruzione in atti giudiziari)
	Art. 319 quater c.p. - (Induzione indebita a dare o promettere utilità)
	Art. 320 c.p. - (Corruzione di persona incaricata di un pubblico servizio)
	Art. 321 c.p. - (Pene per il corruttore)
	Art. 322 c.p. - (Istigazione alla corruzione)
	Art. 322 bis c.p. - (Peculato, concussione, induzione a dare o a promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri)
Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti e segni di riconoscimento (art. 25-bis)	Art. 346 bis c.p. - (Traffico di influenze illecite)
	Art. 453 c.p. - (Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate)
	Art. 454 c.p. - (Alterazione di monete)
	Art. 455 c.p. - (Spendita e introduzione nello Stato, senza concerto, di monete falsificate)
	Art. 457 c.p. - (Spendita di monete falsificate ricevute in buona fede)
	Art. 459 c.p. - (Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati)
	Art. 460 c.p. - (Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo)
	Art. 461 c.p. - (Fabbricazione o detenzione di filigrana o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata)
	Art. 464 c.p. - (Uso di valori di bollo contraffatti o alterati)
	Art. 473 c.p. - (Contraffazione, alterazione o uso di marchi o segni distintivi ovvero brevetti, modelli e disegni)
Delitti contro l'industria e il commercio (art.25-bis.1)	Art. 474 c.p. - (Introduzione nello Stato e commercio di prodotti con segni falsi)
	Art. 513 c.p. - (Turbata libertà dell'industria o del commercio)
	Art. 513 bis c.p. - (Illecita concorrenza con minaccia o violenza)
	Art. 514 c.p. - (Frodi contro le industrie nazionali)
	Art. 515 c.p. - (Frodi nell'esercizio del commercio)
	Art. 516 c.p. - (Vendita di sostanze alimentari non genuine come genuine)
	Art. 517 c.p. - (Vendita di prodotti industriali con segni mendaci)
	Art. 517 ter c.p. - (Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale)
Reati societari (art. 25-ter)	Art. 517 quater c.p. - (Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari)
	Art. 2621 c.c. - (False comunicazioni sociali)
	Art. 2621 bis c.c. - (Fatti di lieve entità)
	Art. 2622 c.c. - (False comunicazioni sociali delle società quotate)
	Art. 2625 c.c. - (Impedito controllo)
	Art. 2626 c.c. - (Indebita restituzione dei conferimenti)
	Art. 2627 c.c. - (Illegale ripartizione degli utili e delle riserve)
	Art. 2628 c.c. - (Illecite operazioni sulle azioni o quote sociali o della società controllante)
	Art. 2629 c.c. - (Operazioni in pregiudizio dei creditori)
	Art. 2629 bis c.c. - (Omessa comunicazione del conflitto d'interessi)
	Art. 2632 c.c. - (Formazione fittizia del capitale)
	Art. 2633 - (Indebita ripartizione dei beni sociali da parte dei liquidatori)
	Art. 2635 c.c. - (Corruzione tra privati)
	Art. 2635 bis c.c. - (Istigazione alla corruzione tra privati)
	Art. 2636 c.c. - (Illecita influenza sull'assemblea)
	Art. 2637 c.c. - (Aggiotaggio)
	Art. 2638 c.c. - (Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza)

Norma di riferimento	Reato presupposto
Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali e delitti contro la personalità individuale (artt. 25-quater, 25-quater.1 e 25-quinquies)	Art. 270 c.p. - (Associazioni sovversive)
	Art. 270 bis c.p. - (Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico)
	Art. 270 bis1 c.p. - (Circostanze aggravanti e attenuanti)
	Art. 270 ter c.p. - (Assistenza agli associati)
	Art. 270 quater c.p. - (Arruolamento con finalità di terrorismo anche internazionale)
	Art. 270 quater1 c.p. - (Organizzazione di trasferimenti per finalità di terrorismo)
	Art. 270 quinquies c.p. - (Addestramento ad attività con finalità di terrorismo anche internazionale)
	Art. 270 quinquies.1. c.p. - (Finanziamento di condotte con finalità di terrorismo)
	Art. 270 quinquies.2. c.p. - (Sottrazione di beni o denaro sottoposti a sequestro)
	Art. 270 sexies c.p. - (Condotte con finalità di terrorismo)
	Art. 280 c.p. - (Attentato per finalità terroristiche o di eversione)
	Art. 280 bis c.p. - (Atto di terrorismo con ordigni micidiali o esplosivi)
	Art. 280 ter c.p. - (Atti di terrorismo nucleare)
	Art. 289 bis c.p. - (Sequestro di persona a scopo di terrorismo o di eversione)
	Art. 289 ter c.p. - (Sequestro a scopo di coazione)
	Art. 302 c.p. - (Istigazione a commettere alcuno dei delitti previsti dai Capi primi e secondi)
	Art. 304 c.p. - (Cospirazione politica mediante accordo)
	Art. 305 c.p. - (Cospirazione politica mediante associazione)
	Art. 306 c.p. - (Banda armata)
	Art. 307 c.p. - (Assistenza ai partecipi di cospirazione o di banda armata)
	Art. 2 L. 342/1976 - (Danneggiamento delle installazioni a terra)
	Art. 1 D.L. 15.12.1979 n. 625 conv. con mod. nella L. 6.2.1980 n. 15 - (Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica)
	Art. 2 Convenzione internazionale per la repressione del finanziamento del terrorismo. New York 9.12.1999
	Art. 383 bis c.p. - (Pratiche di mutilazione degli organi genitali femminili)
	Art. 600 c.p. - (Riduzione o mantenimento in schiavitù o in servitù)
	Art. 600 bis c.p. - (Prostituzione minorile)
	Art. 600 ter c.p. - (Pornografia minorile)
	Art. 600 quater c.p. - (Detenzione di materiale pornografico)
	Art. 600 quater.1 c.p. - (Pornografia virtuale)
	Art. 600 quinquies c.p. - (Iniziative turistiche volte allo sfruttamento della prostituzione minorile)
	Art. 601 c.p. - (Iratta di persone)
	Art. 602 c.p. - (Acquisto e alienazione di schiavi)
	Art. 603 bis c.p. - (Intermediazione illecita e sfruttamento del lavoro)
	Art. 609 undecies c.p. - (Aversamento di minorenni)
Reati di abuso di mercato (art. 25-sexies)	Art. 184 D.lgs. 24.2.1998 n.36 - (Abuso di informazioni privilegiate)
	Art. 185 D.lgs. 24.2.1998 n.36 - (Manipolazione del mercato)
Reati di omicidio colposo o lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies)	Art. 589 c.p. - (Uicidio colposo)
	Art. 590 comma 3 c.p. - (Lesioni personali colpose Art. 583 c.p. - Circostanze aggravanti)
Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (art. 25- octies)	Art. 648 c.p. - (Ricettazione)
	Art. 648 bis c.p. - (Riciclaggio)
	Art. 648 ter c.p. - (Impiego di denaro, beni o utilità di provenienza illecita)
	Art.648 quater c.p. - (Autoriciclaggio)
Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25- octies .1)	Art. 493 ter c.p. - (Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti)
	Art. 493 quater c.p. - (Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti)
	Art. 640 ter c.p. - (Frode informatica)
Delitti in materia di violazione del diritto d'autore (art. 25-novies)	Art.171 legge del 22 aprile del 1941, n.633 - (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)
	Art.171 bis legge del 22 aprile del 1941, n.633 - (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)
	Art.171 ter legge del 22 aprile del 1941, n.633 - (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)
	Art.171 septies legge del 22 aprile del 1941, n.633 - (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)
	Art.171 octies legge del 22 aprile del 1941, n.633 - (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)
	Art. 174 quinquies legge del 22 aprile del 1941, n.663 - (Protezione del diritto d'autore e di altri reati connessi al suo esercizio)
Induzione a non rendere dichiarazioni mendaci o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)	Art.174 bis legge del 22 aprile del 1941, n.663 - (Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria)
	Art. 491 bis c.p. - (Documenti informatici)
Delitti informatici e trattamento illecito di dati (art. 24-bis)	Art. 615 ter c.p. - (Accesso abusivo ad un sistema informatico o telematico)
	Art. 615 quater c.p. - (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)
	Art. 615 quinquies c.p. - (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)
	Art. 617 quater c.p. - (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)
	Art. 617 quinquies c.p. - (Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche)
	Art. 635 bis c.p. - (Danneggiamento di informazioni, dati e programmi informatici)
	Art. 635 ter c.p. - (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)
	Art. 635 quater c.p. - (Danneggiamento di sistemi informatici o telematici)
	Art. 635 quinquies c.p. - (Danneggiamento di sistemi informatici o telematici di pubblica utilità)
	Art. 640 quinquies c.p. - (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)
	Art. 1, comma 11 del D.L. 105/2019, convertito da L. 133/2019 - (Violazione delle norme in materia di Perimetro di Sicurezza Nazionale Cibernetica)

Norma di riferimento	Reato presupposto
Delitti di criminalità organizzata (art. 24-ter)	Art. 416 c.p. - (Associazione per delinquere)
	Art. 416-bis c.p. - (Associazione di tipo mafioso anche straniera)
	Art. 416-ter c.p. - (Scambio elettorale politico-mafioso)
	Art. 630 c.p. - (Sequestro di persona a scopo di estorsione)
	Art. 2 legge 18 aprile 1975, n.110 - (Armi e munizioni comuni da sparo)
	Art. 407, comma 2, lettera a), numero 5) c.p.p. - (Delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'art.2 comma terzo delle legge n. 110 del 1975)
	Art. 73 decreto del Presidente della Repubblica 9 ottobre 1990, n. 309 - (Produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope)
Reati ambientali (art. 25-undecies)	Art. 74 decreto del Presidente della Repubblica 9 ottobre 1990, n. 309 - (Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope)
	Art. 452 bis c.p. - (Inquinamento ambientale)
	Art. 452 quater c.p. - (Disastro ambientale)
	Art. 452 quinquies c.p. - (Delitti colposi contro l'ambiente)
	Art. 452 octies c.p. - (Circostanze aggravanti)
	Art. 416 c.p. - (Associazione per delinquere)
	Art. 416 bis c.p. - (Associazione di tipo mafioso anche straniera)
	Art. 452 sexies c.p. - (Traffico e abbandono di materiale ad alta radioattività)
	Art. 727 bis c.p. - (Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette)
	Art. 733 bis c.p. - (Distruzione o deterioramento di habitat all'interno di un sito protetto)
	Art. 1 della Legge 7 febbraio 1992, n.150 - (Commercio internazionale delle specie animali e vegetali in via d'estinzione, nonché commercializzazione e detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica)
	Art. 2 della Legge 7 febbraio 1992, n.150 - (Commercio internazionale delle specie animali e vegetali in via d'estinzione, nonché commercializzazione e detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica)
	Art. 3 della Legge 7 febbraio 1992, n.150 - (Commercio internazionale delle specie animali e vegetali in via d'estinzione, nonché commercializzazione e detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica)
	Art. 3 bis della Legge 7 febbraio 1992, n.150 - (Commercio internazionale delle specie animali e vegetali in via d'estinzione, nonché commercializzazione e detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica)
	Art. 6 della Legge 7 febbraio 1992, n.150 - (Commercio internazionale delle specie animali e vegetali in via d'estinzione, nonché commercializzazione e detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica)
	Art. 137 del d. lgs del 3 aprile 2006, n.152 - (Totale delle acque)
	Art. 103 del d. lgs del 3 aprile 2006, n.152 - (Scarichi sul suolo)
	Art. 104 del d. lgs del 3 aprile 2006, n.152 - (Scarichi nel sottosuolo e nelle acque sotterranee)
	Art. 107 del d. lgs del 3 aprile 2006, n.152 - (Scarichi in reti fognarie))
	Art. 108 del d. lgs del 3 aprile 2006, n.152 - (Scarichi di sostanze pericolose)
	Art. 256 del d.lgs del 3 aprile 2006, n. 152 - (Attività di gestione di rifiuti non autorizzata)
	Art. 257 del d.lgs del 3 aprile 2006, n. 152 - (Bonifica dei siti)
	Art. 258 del d.lgs del 3 aprile 2006, n. 152 - (Violazione degli obblighi di comunicazione di tenuta dei registri obbligatori e dei formulari)
	Art. 259 del d.lgs del 3 aprile 2006, n. 152 - (Traffico illecito di rifiuti)
	Art. 452 quaterdecies c.p. - (Attività organizzata per il traffico illecito di rifiuti)
	Art. 260 bis del d.lgs del 3 aprile 2006, n. 152 - (Sistema informatico di controllo della tracciabilità dei rifiuti)
	Art. 279 del d.lgs del 3 aprile 2006, n. 152 - (Sanzioni)
	Art. 3 della Legge 28 dicembre 1993, n. 549 - (Misure a tutela dell'ozono stratosferico e dell'ambiente)
	Art.8 del decreto legislativo del 6 novembre 2007 n. 202 - (Inquinamento doloso)
	Art.9 del decreto legislativo del 6 novembre 2007 n. 202 - (Inquinamento colposo)
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies)	Art. 22 e art 12 decreto Legislativo 25 luglio 1998, n. 286 - (Impiego di lavoratori irregolari)
Razzismo e xenofobia (art. 25-terdecies)	Art. 604 bis c.p. - (Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa)
Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies) (introdotti con Legge n. 39/2019)	Art. 1 legge 13 dicembre 1989, n. 401 - (Frode in manifestazioni sportive)
	Art. 4 legge 13 dicembre 1989, n. 401 - (Esercizio abusivo di attività di gioco o di scommessa)
Reati tributari (art. 25-quindecies)	Art. 2 Decreto Legislativo 10 marzo 2000, n. 74 - (Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti)
	Art. 3 Decreto Legislativo 10 marzo 2000, n. 74 - (Dichiarazione fraudolenta mediante artifici)
	Art. 8 Decreto Legislativo 10 marzo 2000, n. 74 - (Emissione di fatture o altri documenti per operazioni inesistenti)
	Art. 10 Decreto Legislativo 10 marzo 2000, n. 74 - (Occultamento o distruzione di documenti contabili)
	Art. 11 Decreto Legislativo 10 marzo 2000, n. 74 - (Sottrazione fraudolenta al pagamento di imposte)

Norma di riferimento	Reato presupposto
Contrabbando (art. 25-sexdecies)	Art. 282 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali)
	Art. 283 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nel movimento delle merci nei laghi di confine)
	Art. 284 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nel movimento marittimo delle merci)
	Art. 285 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nel movimento delle merci per via aerea)
	Art. 286 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nelle zone extra-doganali)
	Art. 287 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando per indebito uso di merci importate con agevolazioni doganali)
	Art. 288 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nei depositi doganali)
	Art. 289 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nel cabotaggio e nella circolazione)
	Art. 290 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nell'esportazione di merci ammesse a restituzione di diritti)
	Art. 291 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando nell'importazione od esportazione temporanea)
	Art. 291-bis D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando di tabacchi lavorati esteri)
	Art. 291-ter D.P.R. 23 gennaio 1973, n. 43 - (Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri)
	Art. 291-quater D.P.R. 23 gennaio 1973, n. 43 - (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri)
	Art. 292 D.P.R. 23 gennaio 1973, n. 43 - (Altri casi di contrabbando)
	Art. 293 D.P.R. 23 gennaio 1973, n. 43 - (Equiparazione del delitto tentato a quello consumato)
	Art. 294 D.P.R. 23 gennaio 1973, n. 43 - (Pena per il contrabbando in caso di mancato o incompleto accertamento dell'oggetto del reato)
	Art. 295 D.P.R. 23 gennaio 1973, n. 43 - (Circostanze aggravanti del contrabbando)
	Art. 295-bis D.P.R. 23 gennaio 1973, n. 43 - (Sanzioni amministrative per le violazioni di lieve entità)
	Art. 296 D.P.R. 23 gennaio 1973, n. 43 - (Recidiva nel contrabbando)
	Art. 297 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando abituale)
	Art. 298 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando professionale)
	Art. 299 D.P.R. 23 gennaio 1973, n. 43 - (Contrabbando abituale o professionale secondo il codice penale)
Delitti contro il patrimonio culturale (art. 25-septiesdecies)	Art. 518-bis c.p. - (Furto di beni culturali)
	Art. 518-ter c.p. - (Appropriazione indebita di beni culturali)
	Art. 518-bis c.p. - (Furto di beni culturali)
	Art. 518-octies c.p. - (Falsificazione in scrittura privata relativa a beni culturali)
	Art. 518-novies c.p. - (Violazioni in materia di alienazione di beni culturali)
	Art. 518-decies c.p. - (Importazione illecita di beni culturali)
	Art. 518-undecies c.p. - (Uscita o esportazione illecite di beni culturali)
	Art. 518-duodecies c.p. - (Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici)
Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies)	Art. 518-quaterdecies c.p. - (Contraffazione di opere d'arte)
	Art. 518-sexies c.p. - (Riciclaggio di beni culturali)
Delitti tentati (art. 26)	Art. 518-terdecies c.p. - (Devastazione e saccheggio di beni culturali e paesaggistici)
	I delitti succitati sono puniti anche se commessi nelle forme del tentativo.

1.1.2 Il D.lgs. 231/2001 e il fenomeno corruttivo ex L. 190/2012

La SO.GE.R.T. S.p.A. svolge l'attività di riscossione dei tributi locali che per giurisprudenza consolidata (*ex multis*, Consiglio di Stato, sent. n. 5284 del 2014) deve essere qualificata come pubblico servizio. Pertanto, è evidente che la Società vada considerata quale soggetto incaricato di pubblico servizio, secondo quanto previsto dal nostro ordinamento.

Tale qualifica soggettiva comporta l'applicazione di tutte le disposizioni penalistiche riferite ai predetti soggetti, in particolare dei delitti contro la Pubblica Amministrazione previsti dal Titolo II, del Libro II del Codice Penale.

Questa categoria di reati, come è noto, è stata oggetto di attenzione sul finire della XVI[°] Legislatura, con l'approvazione della Legge 190/2012 e le sue successive specificazioni. Il fine delle riforme attuate era quello di porre rimedio al fenomeno corruttivo, al di là delle singole e specifiche fattispecie di reato.

La SO.GE.R.T. S.p.A. è ben consapevole che il concetto di corruzione inquadrato dalla l. 190/2012 è inteso in senso più ampio rispetto a quello emergente dal D.Lgs. 231/2001, il quale infatti comprende tra i reati presupposto solo alcuni di quelli contro la Pubblica Amministrazione.

Pertanto, al fine di ottenere un Modello Organizzativo specificamente improntato alla prevenzione della corruzione è opportuno dedicare attenzione anche ai reati non normativamente ricompresi tra quelli presupposto per la responsabilità amministrativa degli enti ex D.Lgs. 231/2001:

- **Peculato (art. 314 c.p.)**

Il delitto previsto dal primo comma dell'articolo de quo si configura allorché il pubblico ufficiale o l'incaricato di pubblico servizio, avendo per ragioni d'ufficio o di servizio *“il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria”*. Il delitto di peculato può integrarsi anche nei casi di assenza di danni patrimoniali concretamente apprezzabili, trattandosi infatti di un reato che offende beni giuridici ulteriori quali l'interesse alla legalità, all'imparzialità ed al corretto agire della P.A.

Il secondo comma dell'articolo punisce, per converso, il c.d. “peculato d'uso”, delitto che si verifica nell'ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio si approprii, nelle circostanze succitate, di una *“cosa”* (*res* specifica; il peculato d'uso non può quindi aversi in presenza di condotta appropriativa di denaro inteso quale bene fungibile o di altri beni fungibili) *“al solo scopo di far[ne] uso momentaneo”*, restituendola immediatamente alla sua funzione originaria.

- **Peculato mediante profitto dell'errore altrui (art. 316 c.p.)**

Il reato punisce il pubblico ufficiale o l'incarico di pubblico servizio che, *“nell'esercizio delle sue funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente per sé o per un terzo denaro o altra utilità”*.

Il delitto de quo si differenzia da quello di cui all'art. 314 c.p. in quanto nel caso qui esaminato la “ricezione” o la “ritenzione” da parte del pubblico ufficiale o dell'incaricato di pubblico servizio avviene durante l'esercizio delle sue funzioni,

mediante giovamento dell'errore altrui. L'errore, sull'*an* o sul *quantum debeatur* deve essere spontaneo, preesistente ed indipendente dall'azione del soggetto agente che, consapevole dell'errore, indebitamente (ovverosia in assenza di alcun titolo legittimante) riceve o ritiene la *res*.

- **Abuso d'ufficio (art. 323 c.p.)**

La disposizione in oggetto punisce (fuori dell'ipotesi in cui il fatto costituisca un più grave reato) la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, "*nello svolgimento delle sue funzioni o del servizio, in violazione di norme di legge o regolamento, ovvero omettendo di astenersi*" dinanzi ad un interesse proprio o di un prossimo congiunto o "*negli altri casi prescritti, intenzionalmente procura a sé o altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto*".

I beni giuridici oggetto di tutela sono costituiti dal buon andamento, dall'imparzialità e dalla trasparenza dell'agire amministrativo, lesi da condotte illegittime non ispirate ad interessi pubblici (tutela della *par condicio civium*).

Il vantaggio ingiusto per come richiamato dalla norma deve essere di natura patrimoniale. Per converso, il danno deve essere solo ingiusto, potendo comportare la lesione di una qualsiasi situazione giuridica soggettiva. Tra condotta dell'agente e l'evento causato deve ovviamente sussistere uno stretto nesso causale (si guardi attentamente all'avverbio "*intenzionalmente*").

- **Utilizzazione di invenzioni e scoperte conosciute per ragioni d'ufficio (art. 325 c.p.)**

Il delitto in esame è integrato dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che utilizza, a profitto proprio o altrui, invenzioni, scoperte scientifiche o nuove applicazioni industriali destinate a rimanere segrete e delle quali sia venuto a conoscenza per ragione dell'ufficio o del servizio.

- **Rivelazione ed utilizzazione di segreti d'ufficio (art. 326 c.p.)**

Il reato, che può essere commesso anche nella forma dell'agevolazione colposa, è integrato dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che rivela notizie di ufficio, le quali debbono rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, commettendo il fatto in violazione dei doveri inerenti alle funzioni o al servizio esercitato, o comunque abusando della qualità rivestita, ovvero è integrato dalla condotta del pubblico ufficiale o incaricato di un pubblico servizio che si avvale illegittimamente di notizie di ufficio, le quali debbono rimanere segrete, al fine di procurare a sé o ad altri un indebito profitto patrimoniale o al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto.

- **Rifiuto d'atti d'ufficio. Omissione (art. 328 c.p.)**

Il reato in esame comprende due distinte e autonome fattispecie incriminatrici che disciplinano, la prima, l'indebito rifiuto di un'attività "qualificata", per ragioni di giustizia o di sicurezza pubblica, o di ordine pubblico o di igiene e sanità,

“indifferibile”

e “doverosa” e, la seconda, l'omissione di un atto della pubblica amministrazione espressamente richiesto, con “messa in mora” del funzionario competente alla sua adozione, da parte di chi abbia interesse al suo compimento e la mancata risposta sulle ragioni del ritardo.

- **Interruzione di un servizio pubblico o di pubblica necessità (art. 331 c.p.)**

Il reato in esame è integrato dalle condotte dirette a turbare la regolarità d'un servizio pubblico o di pubblica necessità mediante l'interruzione di esso ovvero mediante la sospensione del lavoro negli stabilimenti, uffici o aziende ovvero del servizio da parte di coloro che esercitano imprese di servizi pubblici o di pubblica necessità.

- **Turbata libertà degli incanti (art. 353 c.p.)**

La norma è posta a tutela della regolarità delle gare della Pubblica Amministrazione, perciò incrimina l'impedimento o il turbamento di una gara o l'allontanamento dalla stessa di concorrenti che siano realizzati attraverso l'uso di mezzi intimidatori (violenza o minaccia) o fraudolenti (doni, promesse, collusioni e mezzi fraudolenti in genere).

L'ambito di applicazione della norma riguarda solo le ipotesi in cui, in qualsiasi forma, si proceda in forma di gara o licitazione privata, il reato presuppone che vi sia stato inizio della procedura di gara, quindi che almeno sia stato pubblicato il bando, e si realizza quando la gara venga impedita, non potendo essere effettuata a causa di uno dei mezzi suddetti ovvero la gara venga turbata, nel senso che ne venga alterato il regolare

svolgimento per influenzarne il risultato rispetto a quello cui si giungerebbe senza l'intervento perturbatore.

Consapevole dell'importanza di prevenire e reprimere i succitati reati, non costituenti presupposto della responsabilità amministrativa in capo agli enti, la SO.GE.R.T. S.p.A. ha inteso improntare le linee guida, le azioni, gli indirizzi ed i programmi definiti dal proprio Modello Organizzativo alla riduzione nella massima misura possibile del rischio di fenomeni corruttivi

1.1.3 Specifiche prescrizioni su antiriciclaggio e ricettazione

Il Decreto Legislativo 21 novembre 2007 n.231 (Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminosi e di finanziamento del terrorismo) all'art. 63 ha esteso l'ambito applicativo della responsabilità da reato degli Enti ai delitti di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita per "qualsiasi tipologia di società". Questa estensione è avvenuta mediante l'introduzione dell'art. 25^{octies} del d.lgs. 231/2001, richiamando la responsabilità da reato degli Enti per i reati suddetti quali disciplinati dagli articoli 648, 648^{bis} e 648^{ter}, 648 ter.1 del Codice Penale. A seguito dell'introduzione dell'articolo 25^{octies}, i reati in oggetto diventano rilevanti anche a livello domestico. Accanto ai destinatari principali previsti dalla normativa, imprese finanziarie indicate all'art.11 (istituti bancari, intermediari finanziari non bancari, assicurazioni, ecc.) ed alle figure professionali

specificate agli art. 12 e 13 e gli altri soggetti di cui all'art. 14, per quanto attiene l'insieme di obblighi antiriciclaggio previsti dal Titolo II (adeguata verifica della clientela, registrazione e segnalazione di operazioni sospette), è in via indiretta assoggettata ogni tipo di impresa, che oltre all'adozione del modello rimane obbligata a garantirne l'aggiornamento con i nuovi reati. La complessiva normativa antiriciclaggio delineata nel D.lgs. 231/2007 interessa in misura diversa le imprese finanziarie e quelle non finanziarie (sia commerciali che industriali).

Ciò si spiega, in virtù del diverso ruolo che il denaro svolge nell'ambito delle imprese finanziarie, da un lato, e di quelle commerciali e industriali, dall'altro: oggetto di attività per le prime, strumento dell'attività per le seconde. Il reinvestimento nel sistema dell'economia legale rappresenta il momento più dannoso del generale processo di riciclaggio (inteso in senso lato) dei capitali illeciti, perché genera gravi squilibri nel mercato, soprattutto attraverso la distorsione del meccanismo di libera concorrenza.

Riguardo ai delitti di cui agli artt. 648^{bis} c.p. e 648^{ter} c.p., 648 ter.1 c.p., lo scopo dell'incriminazione è quello di impedire che gli autori di fatti di reato possano far fruttare i capitali illegittimamente acquisiti, rimettendoli in circolazione come capitali "depurati" e perciò investibili anche in attività economico-produttive legali. In maniera equivalente riguardo alla previsione di cui all'art. 25^{octies} D.lgs. 231/2001, lo scopo è sostanzialmente equivalente, seppur traslato a livello di ente collettivo, e cioè non solo impedire che gli Enti possano essere utilizzati quale strumento per le attività di riciclaggio e rimpiego, e quindi per ostacolare la giustizia, ma anche impedire che gli stessi possano beneficiare nella loro attività, di capitali di provenienza illecita, inquinando così il mercato.

La SO.GE.R.T. S.p.A., pertanto, potrebbe essere individuata, sotto il profilo criminologico, come “impresa strumentalizzata non criminale”. Un Ente, qualsiasi sia la sua natura (commerciale o industriale), pur operando secondo criteri di economicità e privo di un collegamento diretto alla criminalità organizzata, rientra in questa categoria, se il delitto-presupposto del riciclaggio/reimpiego è originato all'esterno dell'Ente.

In questo caso l'Ente è caratterizzato da una colpa di organizzazione tale da consentire l'instaurarsi di collusioni interne. A volte è dato riscontrare una meno grave colpa di reazione, in assenza di vere e proprie collusioni. In tal caso, l'interesse o il vantaggio per l'Ente non sono evidentemente costituiti dalla ricchezza generata dal delitto presupposto riciclata e reimpiegata, ma dal mero vantaggio economico (compenso, commissione, ecc.) derivante dalla specifica operazione posta in essere e del tutto equivalente al vantaggio che deriverebbe da analoga ma regolare operazione.

La tipologia di riciclaggio che può essere attuata dagli Enti non finanziari può essere definita *riciclaggio monetario*. Il *riciclaggio monetario* si caratterizza per la movimentazione materiale del denaro liquido. L'impianto normativo previsto dal D.lgs. 112/2008 risulta prevedere puntuali limitazioni in merito a: trasferimento di denaro contante; utilizzo ed emissione di assegni; utilizzo dei libretti di deposito.

Non è un caso che la prima diffusa risposta dei sistemi normativi statuali ha contemplato, in primo luogo, il divieto di effettuare operazioni per contanti oltre determinati importi.

Oggi costituisce regola generale di contrasto al riciclaggio la drastica riduzione dell'uso di contanti per qualsiasi tipo di transazione di elevato rilievo economico.

A tal proposito, il Personale dovrà adottare tutti gli strumenti e le cautele opportune per garantire la trasparenza e la correttezza delle transazioni commerciali.

In particolare, è obbligatorio che:

- a) gli incarichi conferiti ad eventuali aziende di servizi e/o persone fisiche che curino gli interessi economico/finanziari dell'Ente siano redatti per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite;
- b) siano rispettati scrupolosamente i requisiti minimi fissati e richiesti ai fini della selezione dei soggetti offerenti i beni e/o servizi che l'Ente intende acquisire;
- c) con riferimento all'attendibilità commerciale/professionale dei fornitori e dei consulenti, siano richieste e ottenute tutte le informazioni necessarie.

1.1.4 I reati Ambientali

Il Decreto Legislativo 07.07.2011 n.121, recante disposizioni di “Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123 CE che modifica la direttiva 2005/35/CE, relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni”, adottato in ritardo rispetto ai tempi imposti per il recepimento dalla normativa europea, secondo cui, gli Stati membri dell'Unione Europea, avrebbero dovuto recepirlo entro il 26 dicembre 2010, ha modificato il Decreto Legislativo 231/2001 introducendo come detto, l'art.25-*undecies* che sancisce la responsabilità degli Enti in relazione alla commissione di alcuni reati ambientali.

Tale intervento è importante, perché, per la prima volta, si responsabilizza l'Ente in relazione ad illeciti ambientali, commessi nel suo interesse o a suo vantaggio, e si prevedono a suo carico sanzioni pecuniarie e, per talune fattispecie, sanzioni interdittive.

In particolare il decreto legislativo n. 121/2011, nel disporre un nuovo catalogo di reati ambientali, presupposto idoneo a fondare la responsabilità dell'Ente, introduce, inoltre, due nuove fattispecie penali agli articoli *727-bis* c.p. (Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette) e *733-bis* c.p. (Distruzione o deterioramento di habitat all'interno di un sito protetto). Per cui l'art. 25-*undecies* sancisce la responsabilità degli Enti sia per alcune figure di reato già previste dall'ordinamento penale, sia per quelle introdotte dal decreto.

Possiamo dividere le fattispecie di reato introdotte da questo articolo, per le quali le aziende possono essere chiamate oggi a rispondere, in macro aree:

- Distruzione di specie animali o vegetali protette; deterioramento di habitat protetti;
tratta di specie in estinzione;
- Scarico acque reflue;
- Rifiuti;
- Inquinamento di suolo, sottosuolo, acque;
- Emissioni in atmosfera;
- Sostanze lesive dell'ozono;

- Inquinamento doloso e colposo provocato dalle navi alla qualità delle acque (scarichi di sostanze inquinanti).

Partendo, nell'analisi delle fattispecie richiamate dall'art. 25-*undecies*, da quelle di nuova introduzione, l'articolo 727-*bis* c.p. punisce diverse tipologie di condotte illecite nei confronti di specie animali e vegetali selvatiche protette, ovvero:

- La condotta di chi, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie selvatica protetta, “salvo che il fatto costituisca più grave reato”, dove tale clausola di riserva comporta il prevalere di fattispecie interferenti punite più severamente.
- La condotta di chi, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta.

Il legislatore delegato, peraltro, adeguandosi alle previsioni della direttiva comunitaria, esclude la configurabilità del reato nei casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie, requisiti che devono sussistere contestualmente.

L'art.733-*bis*, invece, punisce la “distruzione o deterioramento di habitat all'interno di un sito protetto”. Tale norma punisce “chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione”. Il comma 3 della disposizione in esame, infine, aggiunge che “ai fini dell'applicazione dell'art. 733-*bis* c.p.” per “habitat all'interno di un sito protetto” si intende qualsiasi habitat di specie per le quali una zona sia classificata come zona a tutela speciale a norma dell'art.4 paragrafi 1 o 2 della direttiva 2009/147/CE o qualsiasi habitat naturale o un habitat di specie per cui un sito sia designato come zona speciale di conservazione a norma

dell'art.4, paragrafo 4, della direttiva 92/43/CE.

Anche tale articolo, come l'art. 727-bis c.p., si apre con la clausola “fuori dei casi consentiti” la quale rinvia alle norme e ai provvedimenti amministrativi che facoltizzano o impongono di tenere la condotta tipica: si pensi, ad esempio, all'attività antincendio con prodotti chimici che interessi un bosco lambito dalle fiamme o al taglio di piante per ragioni di pubblica incolumità. Inoltre, fondano la responsabilità della Società anche i seguenti reati ambientali (già presenti nell'ordinamento penale):

Nel settore dell'inquinamento idrico:

- scarico idrico in violazione delle prescrizioni contenute nell'autorizzazione (art. 137, comma 3, d.lgs. 3 aprile 2006, n.152) e dei limiti tabellari per talune sostanze (art. 137, comma 5 primo periodo, d.lgs. 3 aprile 2006, n.152);
- scarico in acque marine da parte di navi od aeromobili di sostanze o materiali per i quali è imposto il divieto assoluto di sversamento (art. 137, comma 13, d.lgs. 3 aprile 2006, n.152);
- scarico idrico in assenza di autorizzazione o con autorizzazione sospesa o revocata riguardante talune sostanze pericolose (art. 137, comma 2, d.lgs. 3 aprile 2006, n.152);
- scarico idrico in violazione dei limiti tabellari per talune sostanze particolarmente pericolose (art. 137, comma 5 secondo periodo, d.lgs. 3 aprile 2006, n.152);
- scarico sul suolo, nel sottosuolo o in acque sotterranee (art. 137, comma 11, d.lgs. 3 aprile 2006, n.152).

Nel settore della gestione dei rifiuti e dell'inquinamento atmosferico:

- gestione abusiva di rifiuti non pericolosi (art. 256, comma 1 lett. a, d.lgs. 3 aprile 2006, n.152) e deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi (art. 256, comma 6, d.lgs. 3 aprile 2006, n.152);
- gestione abusiva di rifiuti pericolosi (art. 256, comma 1 lett. b, d.lgs. 3 aprile 2006, n.152); realizzazione e gestione di discarica abusiva di rifiuti non pericolosi (art. 256, comma 3, primo periodo, d.lgs. 3 aprile 2006, n.152); miscelazione di rifiuti (art. 256, comma 5, d.lgs. 3 aprile 2006, n.152);
- realizzazione e gestione di discarica abusiva di rifiuti pericolosi (art. 256, comma 3, secondo periodo, d.lgs. 3 aprile 2006, n.152);
- omessa bonifica di sito contaminato da rifiuti non pericolosi (art. 257, comma 1, d.lgs. 3 aprile 2006, n.152) e pericolosi (art. 257, comma 2, d.lgs. 3 aprile 2006, n.152);
- trasporto di rifiuti pericolosi senza formulario e mancata annotazione nel formulario dei dati relativi (art. 258, comma 4 secondo periodo, d.lgs. 3 aprile 2006, n.152);
- spedizione illecita di rifiuti (art. 259, comma 1, d.lgs. 3 aprile 2006, n.152);
- attività organizzate per il traffico illecito di rifiuti (art. 260, d.lgs. 3 aprile 2006, n.152);

- violazione delle prescrizioni in materia di SISTRI (Sistema di Controllo della Tracciabilità dei Rifiuti) (art. 260-*bis*, d.lgs. 3 aprile 2006, n.152);
- inquinamento atmosferico per superamento dei valori limite di emissione e dei valori limite di qualità dell'aria previsti dalla normativa di settore (art. 279, comma 5, d.lgs. 3 aprile 2006, n.152).

Nell'ambito della tratta di specie in via d'estinzione o pericolose per la salute e l'incolumità pubblica è punita l'importazione, l'esportazione, il trasporto ed l'uso illecito di specie animali e il commercio di piante riprodotte artificialmente (art.1 commi 1 e 2, e art. 2 commi 1 e 2, l. 7 febbraio 1992, n. 150) e la detenzione di esemplari vivi di mammiferi e rettili di specie selvatica o provenienti da riproduzioni in cattività che costituiscono pericolo per la salute e l'incolumità pubblica (art. 6 comma 4, l. 7 febbraio 1992, n. 150), nonché la falsificazione o l'alterazione di certificazioni e licenze e l'uso di certificazioni e di licenze falsi o alterati per l'importazione di animali (art. 3-bis, l. 7 febbraio 1992, n. 150);

Nell'ambito della tutela dell'ozono, rientra la violazione delle disposizioni sull'impiego delle sostanze nocive per lo strato di ozono (art.3 comma 6, l.28 dicembre 1993, n. 549);

Infine, nell'ambito dell'inquinamento provocato da navi viene punito lo sversamento in mare da navi, sia colposo che doloso, di sostanze inquinanti da cui derivino danni permanenti o di particolare gravità alla qualità delle acque, a specie animali o vegetali (art. 8 e 9, commi 1 e 2, d.lgs. 6 novembre 2007, n. 202).

Mentre la sanzione pecuniaria è prevista in relazione a tutte le ipotesi per cui è stata configurata la responsabilità della Società ed è diversamente articolata in proporzione alla ritenuta diversa gravità dei reati presupposto previsti nel catalogo di cui all'art. 25-*undecies*, quanto alle sanzioni previste a carico della Società, il legislatore delegato si è avvalso della facoltà, conferitagli nella legge delega, di non ricorrere necessariamente alle sanzioni interdittive previste dal d.lgs.231/2001.

L'applicazione di tali sanzioni, per una durata fissata dalla norma nella misura non superiore a sei mesi, è stata, infatti, riservata soltanto ai casi in cui i reati da cui scaturisce la responsabilità dell'Ente siano quelli previsti rispettivamente:

- Dall'art.137 commi 2, 5 secondo periodo e 11 d.lgs. n. 152/2006;
- Dall'art. 256 comma 3 d.lgs. n. 152/2006;
- Dall'art. 260 d.lgs. 152/2006;
- Dagli artt. 8 commi 1 e 2 e 9 comma 2 d.lgs.202/2001.

Solo in tali ipotesi, dunque, sarà possibile applicare alla persona giuridica le medesime sanzioni in via cautelare.

La norma inoltre ha previsto anche l'applicazione della sanzione più grave tra quelle previste dal d.lgs. n. 231/2001 e cioè quella dell'interdizione definitiva dall'esercizio dall'attività di cui all'art. 16, ma solo in due ipotesi, ossia nell'ipotesi in cui l'Ente o una sua unità organizzativa vengano stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione dei reati di "associazione" finalizzata al traffico illecito di rifiuti (art. 260 d.lgs.

n. 152/2006) e di sversamento in mare doloso di materie inquinanti (art. 8 commi 1 e 2 d.lgs. n. 202/2007).

Si consideri che a seguito della entrata in vigore del decreto legislativo 1 marzo 2018, n. 21, i richiami all'art. 260 del d.lgs n. 152/2006 vanno riferiti all'articolo 452 *quaterdecies c.p.*, in quanto la prima disposizione è trasmigrata interamente nel codice penale a seguito della attuazione del principio della riserva di codice previsto dalla c.d. "Riforma Orlando".

1.1.5 Le sanzioni applicabili

Le sanzioni per gli illeciti amministrativi dipendenti da reato, previste dall'art. 9 del Decreto sono:

1. sanzioni pecuniarie;
2. sanzioni interdittive;
3. confisca;
4. pubblicazione della sentenza.

La sanzione pecuniaria, che consegue sempre al riconoscimento della responsabilità della Società, viene applicata con il sistema delle quote, come disposto dall'art. 11. Il giudice è chiamato ad effettuare un giudizio, volto a determinare autonomamente: i) il numero delle “quote”, calcolato in ragione della gravità del fatto e del comportamento (antecedente e successivo) assunto dalla Società, e ii) l'importo unitario della singola quota, fissato in ragione delle condizioni economico-patrimoniali dell'Ente stesso, allo scopo esplicito di “assicurare l'efficacia della sanzione”.

Le sanzioni interdittive sono state invece previste in quanto capaci di incidere profondamente sull'organizzazione, sul funzionamento e sull'attività della Società. Affinché possano essere irrogate, però, è necessaria la loro espressa previsione in relazione alle singole tipologie di reato, nonché una particolare gravità del fatto, fondata sul disvalore dell'illecito “amministrativo”, ovvero sulla “pericolosità” della Società stessa, che, in presenza di una reiterazione degli illeciti, ha dimostrato di essere insensibile alle sanzioni pecuniarie (art. 13).

In particolare, le sanzioni interdittive, (ex art. 9, secondo comma) sono:

1. l'interdizione dall'esercizio delle attività;

2. la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
3. il divieto di contrarre con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
4. l'esclusione da agevolazioni, finanziamenti, contributi e sussidi, nonché la revoca di quelli eventualmente già concessi;
5. il divieto di pubblicizzare beni o servizi.

Ai sensi dell'articolo 15 del Decreto, nel caso in cui sussistano i presupposti per l'applicazione di una misura interdittiva che determini l'interruzione dell'attività della Società, il giudice ne dispone il commissariamento ogniqualvolta:

- l'Ente svolge un pubblico servizio o un servizio di pubblica necessità, la cui interruzione può provocare un grave pregiudizio alla collettività;
- ovvero l'interruzione dell'attività della Società possa provocare rilevanti ripercussioni sull'occupazione.

Il tenore afflittivo di questo “*armamentario*” sanzionatorio è ulteriormente accresciuto dalla possibilità, prevista per le sanzioni interdittive e per il c.d. commissariamento, di anticiparne l'applicazione, se pur solo provvisoriamente, quali misure cautelari, già nella fase delle indagini preliminari.

Tanto nel caso di irrogazione di pene pecuniarie che in quello di pene interdittive, l'orientamento “preventivo” del sistema complessivamente delineato dal Decreto si evince dal

fatto che tanto l'attività riparatoria quanto la regolarizzazione "post factum" da parte della

Società coinvolta consentono di diminuire il “quantum” della sanzione pecuniaria, ai sensi dell’art.12, ovvero di escludere l’applicazione di sanzioni interdittive, ex art. 17.

La confisca del prezzo o del profitto del reato, ovvero per equivalente, viene sempre disposta con la sentenza di condanna, salvo che per la parte che può essere restituita al danneggiato, ai sensi dell’art. 19 del Decreto.

La pubblicazione della sentenza può essere disposta solo, nel caso in cui, nei confronti della Società venga applicata una sanzione interdittiva (art. 18 del Decreto).

Quanto alle norme processuali, il Decreto Legislativo in esame prevede che, competente all’accertamento dell’illecito nonché all’applicazione delle sanzioni amministrative *de quibus* sia lo stesso Giudice penale chiamato a verificare la sussistenza dei reati cosiddetti presupposto (artt. 34 e seguenti D.lgs. n. 231 del 2001).

Come è stato già anticipato, nel corso delle indagini è prevista la possibilità di applicare, nei confronti della Società, misure cautelari interdittive, nelle forme del contraddittorio anticipato, nonché il sequestro preventivo e/o conservativo (artt. 45 e seguenti D.lgs. n. 231 del 2001).

1.1.6 Responsabilità della Società e vicende modificative

Il Decreto prevede che, in caso di trasformazione della Società, resti ferma la responsabilità della Società trasformata per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto.

In caso di fusione della Società, anche per incorporazione, la Società che ne risulta risponde dei reati dei quali si siano resi responsabili le Società partecipanti alla fusione, ed allo stesso

saranno applicate le sanzioni pecuniarie e interdittive per gli illeciti amministrativi dipendenti da tali reati.

In caso di scissione parziale, la Società scissa rimane responsabile per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto e la responsabilità solidale delle società beneficiarie si aggiunge a quella della società scissa. In caso di scissione totale, le società o Enti beneficiari della scissione rispondono (in solido tra loro) della sanzione pecuniaria per gli illeciti amministrativi commessi, anteriormente alla scissione, dalla Società scissa. Nella scissione sia totale che parziale, ciascuna Società o Ente beneficiario della scissione risponde nei limiti del patrimonio netto ad essa trasferito. Risponde dell'obbligazione pecuniaria oltre tale limite, se necessario, la Società o Ente a cui sia stato trasferito, anche solo in parte, il ramo di attività nell'ambito del quale è stato commesso il reato. Le sanzioni interdittive relative ai reati commessi anteriormente alla data dalla quale la scissione ha avuto effetto si applicano ai soli Enti ai quali è rimasto (ipotesi riferibile alla sola scissione parziale) ovvero è stato trasferito (in tutti i casi di scissione), anche soltanto in parte, il ramo di attività nel cui ambito è stato commesso il reato.

In caso di cessione dell'azienda nella cui attività è stato commesso il reato, il cessionario è solidalmente obbligato al pagamento della sanzione pecuniaria (salvo il beneficio della preventiva escussione del cedente, e nei limiti del valore dell'azienda ceduta). Il cessionario è tenuto a pagare le sanzioni pecuniarie a condizione che il debito risulti dai libri contabili obbligatori e che il cessionario sia, comunque, a conoscenza degli illeciti amministrativi antecedentemente commessi. Lo stesso vale nelle ipotesi di conferimento d'azienda. Non si applicano, in ogni caso, al cessionario le sanzioni interdittive.

1.1.7 L'adozione del Modello Organizzativo, quale circostanza esimente della responsabilità amministrativa da reato

L'articolo 6 del Decreto prevede, comunque, una specifica esimente dalla responsabilità amministrativa da reato, per cui l'Ente non è responsabile e quindi non può incorrere nelle predette sanzioni, qualora dimostri che:

1. l'Organo Dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto illecito, modelli di organizzazione e gestione idonei a prevenire la realizzazione degli illeciti penali considerati (cd. Modello Organizzativo);
2. abbia affidato, ad un organismo interno all'Ente dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'efficace osservanza del Modello in questione, nonché di curarne l'aggiornamento;
3. le persone che hanno commesso il reato abbiano eluso fraudolentemente il Modello di Organizzazione e Gestione;
4. non vi sia stato omesso o insufficiente controllo da parte dell'Organismo di Vigilanza (di seguito anche "OdV").

Se è vero, insomma, che dalla commissione di uno dei reati di cui sopra può discendere una responsabilità a carico dell'Ente, è altrettanto vero che simile responsabilità ricorre solo allorché all'Ente stesso possa imputarsi una c.d. '*colpa di organizzazione*', vale a dire la mancata istituzione e messa in opera di un organismo di controllo interno, nonché, più in generale, la mancata adozione ed attuazione di un nucleo di regole preventive (per l'appunto, il

Modello Organizzativo di cui sopra), volte a prevenire o contrastare l'eventuale agire illecito dei soggetti apicali e subalterni.

Un'ulteriore precisazione è ricavabile dagli artt. 6 e 7 D.lgs. 231/2001: se il fatto è stato commesso da amministratori, dirigenti, rappresentanti o preposti, la colpa d'organizzazione si presume e spetta dunque all'Ente provarne l'insussistenza; se invece il fatto è stato commesso da dipendenti, la colpa d'organizzazione va provata da parte di chi invece (nel processo penale, il pubblico ministero) ne sostiene il ricorrere.

Il Decreto prevede (art. 6), inoltre, che i modelli di organizzazione e gestione debbano rispondere alle seguenti esigenze di efficace ed efficiente attuazione:

1. individuare le attività nel cui ambito possono essere commessi i reati;
2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
4. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
5. introdurre un Sistema Disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
6. prevedere uno o più canali che consentano, in riservatezza, ai soggetti apicali o dipendenti di segnalare condotte illecite rivelanti ai sensi del Decreto 231/2001 poste essere all'interno dell'Ente, o violazioni del presente Modello Organizzativo

La formulazione delle regole cautelari e delle procedure che devono confluire nel modello di organizzazione e gestione dell'attività della SO.GE.R.T. S.p.A. deve, non solo assicurare la prevenzione dei fatti di reato da parte dei soggetti responsabili nell'esercizio delle loro funzioni, ma anche regolare l'opportuna azione di controllo da parte dell'Organismo di Vigilanza, in riferimento al fondamentale criterio di assicurare un giudizio di idoneità da parte dell'autorità giudiziaria, che conduca all' "esonero" di responsabilità dell'Ente. Detta efficacia esonerante non potrà essere raggiunta se non a seguito dell'adozione dei protocolli preventivi.

1.1.8 La costruzione del Modello di Organizzazione, Gestione e Controllo

In un quadro siffatto, la messa a punto, l'adozione e l'applicazione del "Modello Organizzativo" rappresenta, se non un vero e proprio obbligo giuridico, quanto meno un onere (dovere libero) ed una necessità per gli Enti che vogliano operare con la ragionevole certezza di non essere coinvolti nel meccanismo sanzionatorio previsto dal decreto.

È altrettanto chiaro, tuttavia, che la disciplina dettata dal D.lgs. n. 231/2001 chiama in causa tutti i dipendenti e gli operatori degli Enti. Nei loro confronti, anzi, il rispetto delle procedure e dei principi indicati dal modello rappresenta un obbligo imprescindibile, il cui pieno e leale assolvimento essi sono tenuti a garantire per almeno due ragioni. La prima è che, in quanto aventi ad oggetto, più o meno direttamente, il patrimonio o l'immagine dell'Ente, le sanzioni previste dal D.lgs. 231/2001 possono produrre danni economici che si riverberano sulla capacità dello stesso di creare ricchezza ed opportunità di lavoro. La seconda è che il rispetto dei principi

ispiratori del Modello è parte integrante di un'immagine che chiunque agisca in nome e per conto dell'Ente è tenuto a garantire.

Ciò premesso si indicano alcuni **requisiti essenziali del Modello Organizzativo**.

Il Legislatore ha individuato i criteri essenziali che i modelli di organizzazione e gestione per la prevenzione dei reati disciplinati dal Decreto devono possedere per essere valutati idonei a determinare l'esclusione della responsabilità dell'Ente ed ha imposto all'Organo dirigente, ai fini indicati nell'art. 6 del Decreto, l'adozione e l'efficace attuazione di tali modelli.

Ulteriori prescrizioni in tal senso sono dettate, in materia di sicurezza ed igiene sul lavoro, dall'art.30 T.U. n. 81 del 9 aprile 2008¹, che introduce ulteriori requisiti di idoneità del Modello

¹ **Art. 30 D. lgs. n. 81/08 :**

1. *Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di responsabilità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:*
 - a) *Al rispetto degli standard tecnico – strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici, biologici;*
 - b) *Alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;*
 - c) *Alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;*
 - d) *Alle attività di sorveglianza sanitaria;*
 - e) *Alle attività di informazione e formazione dei lavoratori;*
 - f) *Alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;*
 - g) *Alla acquisizione di documentazioni e certificazioni obbligatorie di legge;*
 - h) *Alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.*
 2. *Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.*
 3. *Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.*
 4. *Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.*
 5. *In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI – INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per la parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'art. 6.*
- 5bis. *La commissione consultiva permanente per la salute e sicurezza sul lavoro elabora procedure semplificate per la adozione e la efficace attuazione dei modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali.*
- L'adozione del modello di organizzazione e di gestione di cui al presente articolo nelle imprese fino a 50 lavoratori rientra tra le attività finanziabili ai sensi dell'art. 11.*

di organizzazione e gestione ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche in relazione ai reati di cui all'art. 25^{septies} del Decreto.

Ne discende che ad oggi può considerarsi efficace, anche alla luce delle pronunce giurisprudenziali, un Modello Organizzativo, adeguato ai sensi del Decreto, se contiene le seguenti componenti essenziali:

- A) principi di comportamento idonei a prevenire la commissione delle fattispecie di reato contemplate dal Decreto capaci di assicurare:
 - l'osservanza delle leggi e dei regolamenti vigenti;
 - il rispetto dei principi di correttezza e trasparenza nei rapporti dell'Ente con la Pubblica Amministrazione e con i terzi;
 - l'attenzione degli operatori sul puntuale rispetto delle procedure di controllo.
- B) costituzione dell'Organismo di Vigilanza e attribuzione allo stesso di specifici compiti di vigilanza sull'efficace, effettivo e corretto funzionamento del Modello;
- C) mappatura delle attività dell'Ente "sensibili", ovvero delle attività nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto, da sottoporre pertanto ad analisi e costante monitoraggio;
- D) definizione dei "protocolli" finalizzati a garantire, nell'ambito delle attività dell'Ente "a rischio", i seguenti principi di controllo:
 - separazione di funzioni, all'interno di ciascun processo, per cui l'impulso decisionale, l'esecuzione, la conclusione ed il controllo di ogni operazione devono essere attribuiti a soggetti diversi. Il principio della separazione delle

funzioni consente la chiara attribuzione delle responsabilità e dei poteri di rappresentanza, nel rispetto delle linee gerarchiche;

- definizione e regolamentazione delle modalità e tempistiche di svolgimento delle attività all'interno di ciascun processo;
- tracciabilità e comprovabilità dei processi ovvero degli atti, delle operazioni e delle transazioni attraverso adeguati riscontri documentali che attestino i contenuti e le motivazioni dell'operazione ed individuino i soggetti a vario titolo coinvolti nell'operazione (autorizzazione, effettuazione, registrazione, verifica dell'operazione);
- oggettività dei processi decisionali al fine di limitare decisioni dell'Ente basate su scelte soggettive non legate a predefiniti criteri oggettivi (es.: esistenza di albi fornitori, esistenza di criteri oggettivi di valutazione e selezione del personale, o esistenza e documentazione di attività di controllo e supervisione, compiute sulle transazioni dell'Ente, ecc.);

E) chiara e formalizzata assegnazione dei poteri e delle relative responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa. In particolare, tutti coloro che intrattengono rapporti con la Pubblica Amministrazione per conto dell'Ente devono essere dotati di delega formale; le deleghe devono associare il potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma;

- F) aggiornamento costante delle deleghe, in conseguenza dei mutamenti organizzativi intervenuti²;
- G) definizione di flussi informativi nei confronti dell'Organismo di Vigilanza;
- H) previsione di canali che consentano agli organi apicali e al personale sottoposto di segnalare in assoluta riservatezza la presunta commissione, all'interno dell'Ente, di illeciti rilevanti ai sensi del Decreto 231/2001 ovvero violazioni del Modello Organizzativo, garantendo loro da condotte discriminatorie o ritorsive per motivi collegati alla segnalazione;
- I) definizione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- J) attività di formazione e diffusione a tutti i livelli societari delle regole comportamentali e delle procedure istituite.

1.2 La tutela del Whistleblower

Il 29 dicembre 2017 è entrata in vigore la legge n. 179 recante “Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato”.

La legge mira a incentivare la collaborazione dei lavoratori per favorire l'emersione dei fenomeni corruttivi all'interno di enti pubblici e privati. L'introduzione di una disciplina ad hoc

² la delega deve definire in modo specifico e certo i poteri del delegato, quelli del soggetto al quale il delegato stesso si rapporta, anche al fine di consentire una adeguata vigilanza sul suo operato; il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli; è necessaria l'esistenza di regole comportamentali idonee a garantire l'esercizio delle attività dell'Ente nel rispetto delle leggi e dei



regolamenti e dell'integrità del patrimonio dell'Ente.

sul fenomeno del c.d. whistleblowing recepisce l'invito a rafforzare l'azione di prevenzione e contrasto di reati commessi in ambito aziendale, anche con la previsione di sistemi che consentono ai lavoratori di segnalare in condizioni di sicurezza gli eventuali illeciti di cui vengono a conoscenza.

Tale finalità ben si concilia con il precipuo scopo del D.lgs. 231/2001 di prevenire la commissione di illeciti penali all'interno di una compagine sociale attraverso l'adozione di un idoneo Modello Organizzativo.

Infatti, l'articolo 2 della legge n. 179/17 interviene sul decreto 231 e, integrando l'articolo 6³ con i commi 2bis, 2ter e 2quater, inserisce una nuova previsione che inquadra nell'ambito del Modello Organizzativo le misure legate alla presentazione e gestione delle segnalazioni.

Alla luce di questo intervento normativo, il Modello Organizzativo risulterà idoneo allorché avrà previsto canali in grado di consentire ai soggetti apicali e a coloro che sono da questi diretti o controllati di presentare, a tutela della integrità dell'Ente, segnalazioni circostanziate di

³ **Art. 6, comma 2bis, del D.lgs. 231/2001:**

"I modelli di cui alla lettera a) del comma 1 prevedono:

a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

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

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

d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate".

Art. 6, comma 2ter, del D.lgs. 231/2001:

"L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2bis può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo".

Art. 6, comma 2quater, del D.lgs. 231/2001:

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

condotte illecite rilevanti in materia di responsabilità amministrativa da reato degli enti, fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del Modello Organizzativo.

I canali dovranno garantire la riservatezza dell'identità del segnalante ed il Modello Organizzativo dovrà evitare che nei confronti di quest'ultimo soggetto vengano perpetrati atti di ritorsione o di discriminazione per il fatto della segnalazione.

1.2.1 Specifiche prescrizioni in materia di Whistleblowing

Nel paragrafo precedente si è analizzata genericamente la modifica apportata all'art. 6 del Decreto 231/2001 con cui si è introdotto l'obbligo, per le società che si dotano di un Modello Organizzativo, di tutelare il "Whistleblower" e dunque di incentivare l'attività di segnalazione. Di seguito le *best practices* da seguire per imprimere maggiore effettività alle nuove prescrizioni.

- A) Il legislatore ha individuato negli apicali e nei sottoposti quei soggetti che possono effettuare segnalazioni. Tale indicazione, animata dal probabile intento di evitare una copiosa proliferazione di segnalazioni, non deve portare a ritenere esistente un *numerus clausus*: la *ratio legis* non esclude la possibilità che altri soggetti esterni alla società segnalino. Infatti, se così non fosse, il novero di persone potrebbe risultare, nella concretezza delle diverse forme di organizzazione, eccessivamente ristretto. Basti pensare, ad esempio, che molteplici sono le realtà organizzative, con personale numericamente esiguo, che intrattengono rapporti con Istituzioni e cittadini – utenti. In

tali ipotesi, non remote, limitare l'elenco dei potenziali segnalanti ai soli apicali e sottoposti potrebbe rendere inefficace, sul punto, il Modello Organizzativo.

È opportuno, conseguentemente, che si dia la possibilità di segnalare anche a soggetti che entrano a contatto con l'Ente in ragione del suo oggetto sociale. Questi ultimi devono essere messi a conoscenza di tale possibilità e degli strumenti all'uopo predisposti, nonché dei rischi derivanti da segnalazioni con carattere temerario.

- B) Oggetto delle segnalazioni sono le “condotte illecite” rilevanti ai sensi del Decreto e le “violazioni del Modello Organizzativo”.

Le prime devono essere “circonstanziate”, oltretutto “fondate su elementi di fatto precisi e concordanti”: tali locuzioni stanno a significare come, in sostanza, nel convincimento del Whistleblower i fatti segnalati debbano integrare le fattispecie di reato richiamate nel Decreto e poter ragionevolmente essere provati.

Le violazioni del Modello Organizzativo, per converso, consistono in violazioni di regole poste dallo stesso e che non necessariamente integrano fattispecie di reato.

- C) I requisiti naturali dell'organo deputato a ricevere la segnalazione sono costituiti dall'indipendenza e dai poteri di azione: tali caratteristiche consentono di prevenire, conoscere, reprimere illeciti e violazioni. È opinione valida e diffusa quella secondo cui le segnalazioni ben possono essere rivolte all'ODV e da questo evase.

Sul punto, prendendo atto delle forme diverse di organizzazione, il legislatore ha comunque lasciato il singolo Ente libero di individuare un altro organismo, dotato di indipendenza e di pieni poteri, purché rimangano garantiti i canali di comunicazione e

la tutela del segnalante. In quest'ultimo caso, permangono ovviamente saldi gli obblighi discendenti dal flusso informativo con l'ODV.

D) I canali di segnalazione devono essere almeno due e uno obbligatoriamente di carattere informatico.

Le caratteristiche del mezzo di trasmissione si intrecciano necessariamente con la tutela della riservatezza della identità dell'agente. Il legislatore non ha espressamente previsto la modalità di segnalazione in forma anonima, tuttavia si ritiene che se il fine precipuo della innovazione è la prevenzione e la repressione degli illeciti, la segnalazione anonima deve vedere riconosciuta la propria dignità. Per evitare inutili proliferazioni, segnalazioni temerarie o dolose si dovranno prevedere dei filtri in entrata, circostanziando maggiormente le denunce, ovvero prendere in considerazione solo quelle che avranno visto un dialogo anonimo col soggetto Whistleblower, come si vedrà. Dopo un'attenta analisi comparata, lo strumento informatico appare l'unico in grado di bilanciare la tutela della riservatezza e l'adeguatezza nel trattare la segnalazione, anonima o meno che sia: la posta ordinaria o il fax infatti, pur potendo astrattamente garantire la riservatezza, lasciano dubbi relativamente al secondo aspetto.

Deve guardarsi in maniera sfavorevole alle segnalazioni che possono essere rese unicamente utilizzando computer ad hoc posti all'interno dei locali appartenenti all'ente: si tratta di un evidente disincentivo alla segnalazione che non merita ulteriori

approfondimenti. Il canale informatico deve essere pertanto accessibile anche da smartphone o pc personali.

Per la buona evasione della segnalazione andrebbe consentito ed incentivato un dialogo riservato tra il Whistleblower e l'organo deputato a ricevere la comunicazione e quindi ad attivarsi. Infatti il solo contatto occorso in sede di segnalazione potrebbe non essere sufficiente.

Lo scambio di informazioni può aversi sia nel caso in cui il soggetto si identifichi, sia nel caso in cui scelga di rimanere anonimo.

La tecnologia odierna vede l'esistenza di piattaforme (app., siti internet; si veda anche quanto predisposto dall'ANAC) che consentono al segnalante anonimo di interloquire in più fasi con l'altra parte per il mezzo di sistemi crittografati che danno vita a quella che può essere certamente definita una chat.

Nel caso più semplice in cui invece debba semplicemente essere garantita la riservatezza dei dati del segnalante, tale funzione può ritenersi efficacemente attuata mediante

caselle di posta elettronica dedicata le cui credenziali siano nell'esclusivo possesso dell'organo indipendente.

Ovviamente, i canali di segnalazione devono essere adeguatamente pubblicizzati, soprattutto nei confronti dei soggetti esterni all'organigramma dell'Ente.

- E) I modelli debbono altresì prevedere sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua segnalazioni in mala fede o versando in colpa grave.

Ulteriori previsioni inerenti al sistema del Whistleblowing saranno analizzate nel corpo del Regolamento dell'ODV e nei paragrafi legati alla formazione.

2. Il Modello di Organizzazione, Gestione e Controllo predisposto dalla SO.GE.R.T. S.p.A.

Nel panorama dei progetti per la gestione dei tributi locali la SO.GE.R.T. S.p.A. svolge attività di riscossione, liquidazione, accertamento, comprese le fasi coattive, delle entrate tributarie ed extratributarie, incluse le sanzioni a qualsiasi titolo emesse, di spettanza degli Enti locali ai sensi dell'art. 52 del D.Lgs. 15 dicembre 1997 n. 446 nonché servizi integrativi ed ausiliari alla attività di riscossione stessa.

In particolare le attività svolte dalla SO.GE.R.T. S.p.A. si possono così sinteticamente elencare:

- Accertamento dei tributi locali e riscossione dei tributi per conto degli Enti locali (Comuni, Consorzi, eccetera);

- Riscossione dell'Imposta comunale sugli immobili (ICI), della Tassa Rifiuti Solidi Urbani (TARSU) e della Tariffa Igiene Ambientale (TIA) per conto dei Comuni;
- Riscossione acqua, acque reflue, depurazione ed eccedenza;
- Riscossione dei contributi imposti dai Consorzi di Bonifica;
- Riscossione delle sanzioni per violazioni al Codice della strada;
- Riscossione coattiva a mezzo ingiunzione fiscale secondo le procedure disciplinate dal R.D. n. 639/1910;
- Attività di stampa e notifica dell'avviso di pagamento contenente il debito dovuto;
- Fornitura di servizi connessi alla riscossione locale (servizi WEB, prodotti informatici, eccetera);
- Attività e servizi in favore degli Enti Locali (riscossione, rendicontazione incassi, acquisizione ottica, eccetera);
- Presenza sul territorio con sportelli nonché predisposizione di canali di riscossione maggiormente innovativi, quali internet, per permettere ai contribuenti di eseguire i versamenti con modalità e forme ispirate al principio della comodità e della economicità;
- Servizio di Tesoreria complesso di operazioni relative alla gestione finanziaria dell'Ente, finalizzate alla riscossione delle entrate, al pagamento delle spese, alla custodia dei titoli e valori ed a tutti gli adempimenti previsti dalla legge, dallo statuto, dai regolamenti dell'Ente.

La SO.GE.R.T. S.p.a. è inserita nell'elenco delle Imprese con Rating di Legalità così come previsto dall'art. 8 del Regolamento adottato dall'Autorità Garante della Concorrenza e del Mercato. La SO.GE.R.T. S.p.A. ha Sede Legale a Grumo Nevano (NA).

La società è controllata al 100% dalla Famiglia Coppola.

Il Dott. Giuseppe Coppola è il Presidente del Consiglio d'Amministrazione, mentre la sorella Dot.ssa Olga Coppola riveste il ruolo di Amministratore Delegato.

Al padre Domenico Coppola spetta la Direzione Generale della Società, nonché la Direzione Tecnica in aggiunta alla sua carica di Consigliere di Amministrazione.

La società risulta iscritta al Registro delle Imprese di Napoli dal 19 febbraio 1996 al n.ro 05491900634.

La Società ha chiuso l'esercizio 2020 con un capitale sociale pari a Euro 10.000.000,00, un patrimonio netto pari a Euro 12.030.971,00 ed un utile pari a circa Euro 254.396,00.

In uno scenario di questo tipo, risulta quanto mai opportuno procedere all'adozione di un Modello Organizzativo capace di assicurare le giuste condizioni di correttezza e trasparenza nella conduzione delle attività della Società, in linea con le prescrizioni del Decreto Legislativo. SO.GE.R.T. S.p.A. ritiene che, con l'adozione di tale Modello, unitamente all'emanazione ed adozione di un Codice Etico, si introduca, nella realtà della Società, l'opportuno strumento di sensibilizzazione di tutti i Dipendenti, Collaboratori e di tutti gli altri soggetti alla stessa cointeressati, tra cui sicuramente vanno annoverati, soprattutto le istituzioni comunali, provinciali e nazionali, nonché, cittadini, clienti, fornitori, le associazioni di categoria, le associazioni ambientali.

Tutto ciò affinché i suddetti soggetti seguano, nella realizzazione delle proprie attività, comportamenti corretti conformi ai principi cui si ispira la SO.GE.R.T. S.p.A., nel perseguimento del proprio oggetto sociale, e tali comunque da prevenire il rischio di commissione dei reati contemplati nel Decreto.

In particolare, l'adozione e la diffusione del Modello mira, da un lato a determinare una piena consapevolezza nel potenziale autore del reato di commettere un illecito, dall'altro, grazie ad un costante monitoraggio dell'attività, a consentire alla SO.GE.R.T. S.p.A. di prevenire o reagire tempestivamente al fine di impedire la commissione del reato stesso.

La SO.GE.R.T. S.p.A. dunque, intende adottare ed attuare efficacemente il Modello, non solo ai fini dell'esimente prevista dal D.lgs. 231/01, ma anche per migliorare la propria *Corporate Governance*, limitando il rischio di commissione dei reati.

2.1 Finalità del Modello

Le finalità del Modello sono quelle di

- Determinare, in tutti coloro che operano in nome e per conto della Società, soprattutto nelle medesime Aree a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'Ente;
- Ribadire che tali forme di comportamento illecito sono fortemente condannate da SO.GE.R.T. S.p.A. in quanto (anche nel caso in cui SO.GE.R.T. S.p.A. fosse

apparentemente in condizioni di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico sociali cui intende attenersi nell'espletamento della propria missione aziendale;

- Intervenire tempestivamente per prevenire, contrastare o ragionevolmente limitare, grazie ad una efficace azione di monitoraggio, i possibili rischi connessi all'attività della Società con particolare riguardo alla eliminazione o significativa riduzione di eventuali condotte illegali.

Scopo del Modello è pertanto la predisposizione di un sistema strutturato, integrato e organico di prevenzione, dissuasione e controllo, finalizzato alla riduzione del rischio di commissione dei reati anche mediante l'individuazione di "attività sensibili" e, ove necessario, la loro conseguente corretta procedimentalizzazione.

Pertanto, il Modello predisposto dalla Società si fonda su un sistema strutturato di procedure organizzative operative e di attività di controllo che quindi, nella sostanza:

1. sono basate sull'individuazione delle aree e dei processi della Società che presentano macro criticità, tali da ingenerare possibili situazioni a rischio-reato nell'attività della Società, con particolare riguardo a quelle che comportano un rischio reato ai sensi del Decreto, secondo criteri che consentano di valutarne, verificarne e documentarne l'impatto economico – cd. *Risk Assessment*;
2. costituiscono un sistema normativo interno diretto a formalizzare l'adozione e l'attuazione delle procedure decisionali all'interno della Società in relazione ai rischi/reati da prevenire tramite:

- il sistema normativo dei Protocolli, in cui confluisce anche il Codice Etico, che a sua volta fissa le linee di orientamento programmatiche tali da assicurare l'efficiente attuazione di procedure operative formalizzate, tese a disciplinare in dettaglio le modalità per assumere e attuare decisioni nelle aree a rischio di commissione dei reati previsti dal Decreto, nonché volti a garantire la documentazione e/o verifica di ogni operazione in dette aree;
 - un sistema di deleghe e di poteri operante all'interno della Società chiaro e trasparente, che consenta di evidenziare con facilità i soggetti coinvolti nei diversi processi di formazione e di attuazione delle decisioni, nel pieno rispetto del citato principio di separazione delle funzioni;
 - la definizione di strutture organizzative coerenti con l'obiettivo di ispirare e controllare la correttezza dei comportamenti, garantendo una chiara e organica attribuzione dei compiti, applicando una reale segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
3. individuano i processi di gestione e controllo delle risorse finanziarie nelle attività potenzialmente a rischio reato;
 4. attribuiscono all'Organismo di Vigilanza specifici compiti di vigilanza sull'efficacia e corretto funzionamento del Modello, sulla coerenza dello stesso con gli obiettivi e sul suo aggiornamento periodico, nonché di curarne la diffusione al personale e ai Collaboratori esterni e ai terzi in genere che intrattengono rapporti, di qualsiasi natura, con la SO.GE.R.T. S.p.A.

2.2 Costruzione del Modello

A far data dal 2016, l'Ente ha deliberato l'avvio di un progetto interno finalizzato alla predisposizione del Modello con il supporto di collaboratori e professionisti esterni con una specifica preparazione nel campo sia del diritto penale commerciale, sia dell'organizzazione aziendale e dei sistemi di controllo interno. A tal fine, SO.GE.R.T. S.p.A. è stata coinvolta in attività propedeutiche suddivise in differenti fasi e dirette tutte all'elaborazione di un sistema di prevenzione e gestione dei rischi, tenendo conto delle *“Linee Guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche”*, salvo che per i necessari adattamenti dovuti alla particolare struttura organizzativa della Società ed alla propria concreta attività.

Con riferimento alle “esigenze” individuate dal legislatore in relazione ai Modelli, i punti fondamentali sviluppati dalle Linee Guida dell'ABI possono essere così brevemente riassunti:

- a) *mappatura delle attività o funzioni aziendali nell'ambito delle quali possono essere commessi i reati, al fine di individuare i presidi da adottare in relazione all'esistenza di rischi concreti di commissione dei reati.*
- b) *previsione di regole dirette a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire (modalità di gestione del rischio) ed individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.*

In particolare, le fasi in cui si è articolato il percorso che ha portato all'individuazione delle aree a rischio, sulla cui base è stato successivamente redatto il Modello, sono state articolate nelle seguenti attività di analisi:

- esame del Modello Organizzativo e di controllo esistente;
- mappatura delle attività a rischio reato ex d.lgs. n. 231/2001;

- specifiche riflessioni sulle previsioni ex l. n. 190/2012;

- definizione dei protocolli etico-comportamentali da implementare;
- pianificazione delle attività di formazione e comunicazione del Modello;
- definizione del Codice Etico;
- definizione delle linee guida relative al funzionamento dell'Organismo di Vigilanza;
- definizione del sistema disciplinare.

2.2.1 Struttura del Modello

Il Modello dunque, così predisposto a seguito delle attività descritte che precedono, è costituito da:

1. **Parte Generale**, che contiene le regole e i principi generali del Modello;
2. **Parte Speciale**, dove sono analizzate le singole fattispecie di reato, e sono definiti i protocolli etico-organizzativi costituiti dalle procedure e dalle regole che, nel dettaglio, devono guidare la dinamica dei processi e dei sistemi di controllo interni all'Ente, ed essere applicati tenendo conto dell'esito dell'analisi in relazione alle possibili modalità di realizzazione dei reati - presupposto;
3. **Mappatura delle Aree di Rischio**, che consente l'individuazione delle aree che risultano interessate dalle casistiche di reato indicate nel D.lgs. 231/01;
4. **Codice Etico**, dove sono prospettati i principi deontologici cui l'attività della SO.GE.R.T. S.p.A. e il Modello stesso sono improntati;
5. **Linee Guida Regolamento dell'Organismo di Vigilanza**, al fine di disciplinare gli

aspetti e le modalità di funzionamento dell'Organo di controllo previsto dal Decreto;

6. **Sistema Disciplinare**, che prevede le sanzioni da irrogare, e le relative procedure applicative.

Il Modello così articolato consente una più efficace e snella attività di aggiornamento dello stesso. La dinamica sociale e l'evoluzione legislativa – quale, ad esempio, una possibile estensione delle tipologie di reati che, per effetto di altre normative, siano inseriti o comunque collegati all'ambito di applicazione del Decreto – potranno rendere, in futuro, necessaria l'integrazione e/o l'aggiornamento del Modello. Ma anche le stesse trasformazioni dell'organico della Società e la quotidiana implementazione del Modello possono suggerire i necessari adeguamenti, al fine di minimizzare i livelli di rischio all'interno della SO.GE.R.T. S.p.A. In considerazione di quanto sopra, l'Organismo di Vigilanza ha il compito di adottare ogni tipo di provvedimento affinché il Consiglio di Amministrazione della SO.GE.R.T. S.p.A. proceda costantemente all'aggiornamento del Modello.

2.2.2 Adozione del Modello nell'ambito della SO.GE.R.T. S.p.A.

Sebbene l'adozione del Modello sia prevista dal Decreto come meramente facoltativa e non obbligatoria, SO.GE.R.T. S.p.A. – in conformità con le proprie politiche – ha comunque ritenuto opportuno procedere alla elaborazione del Modello.

Essendo il Modello atto dell'Organo Dirigente, secondo quanto previsto dall'art. 6, comma 1, lettera a) del d.lgs., le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione, ovvero di un suo delegato, salvo successiva approvazione dello stesso Consiglio in quanto titolare del potere di adozione e modifica del Modello.

2.2.3 Attuazione del Modello all'interno della SO.GE.R.T. S.p.A.

Il Consiglio di Amministrazione della SO.GE.R.T. S.p.A., al fine di assicurare l'efficace applicazione del Modello di Organizzazione, Gestione e Controllo adottato, curerà il coordinamento delle attività di implementazione e verifica dello stesso, nonché proporrà e discuterà le modifiche che si riterranno necessarie, sulla base delle esigenze di adeguamento emerse in sede di verifica.

A tal fine, è attribuito all'Organismo di Vigilanza il compito primario di esercitare il controllo sull'attuazione del Modello stesso, secondo le procedure in esso descritte, e per mezzo dei poteri e delle funzioni di cui lo stesso è investito, secondo il Regolamento proprio dell'Organo di controllo.

Lo stesso Organismo di Vigilanza ha, altresì, il compito di dare impulso e di coordinare in via generale, all'interno della Società, anche mediante contatti sulla rete informatica, le attività di controllo sull'applicazione del Modello, al fine di una sicura, corretta ed omogenea attuazione.

2.2.4 Destinatari del Modello

Le regole contenute nel Modello e nel Codice Etico si applicano in primo luogo a coloro che svolgono funzioni di rappresentanza, amministrazione o direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché a chi esercita anche di fatto la gestione e il controllo della Società.

L'applicazione del Modello e del codice Etico è estesa poi a tutti i dipendenti della SO.GE.R.T. S.p.A., e altresì, nei limiti del rapporto in essere, a coloro i quali pur non



appartenendo alla

Società, operano su mandato e per conto dello stesso o sono comunque legati alla Società da rapporti giuridici rilevanti in funzione della prevenzione dei reati. Il Consiglio di Amministrazione, ovvero un suo delegato, determina preliminarmente le modalità di comunicazione del Modello e del Codice Etico ai soggetti esterni interessati, nonché le procedure necessarie per il rispetto delle disposizioni in essi contenute in modo da assicurarne l'effettiva conoscenza da parte di tutti i soggetti interessati, secondo le modalità stabilite al successivo paragrafo 5.1. I destinatari del Modello e del Codice Etico sono tenuti a rispettare con la massima correttezza e diligenza tutte le disposizioni e i protocolli in essi contenuti, nonché tutte le procedure di attuazione delle stesse.

2.2.5 Il Codice Etico

Parimenti al Modello di Organizzazione, Gestione e Controllo, e quale parte integrante dello stesso, il Consiglio di Amministrazione della SO.GE.R.T. S.p.A. ha adottato il Codice Etico, quale documento ufficiale in cui sono dichiarati i principi e i valori caratteristici della Società, e in cui devono riconoscersi tutti coloro che operano, in essa e per essa.

Esso tende ad uniformare i singoli comportamenti della Società al fine di rendere compatibile e sinergico il fine aziendale perseguito, con le esigenze di legalità sottese all'adozione del d.lgs.

n. 231/2001, e che devono essere anch'esse incorporate nei principi ispiratori della missione e della deontologia della SO.GE.R.T. S.p.A.

Il Codice Etico, dunque, si colloca nell'ambiente di controllo della Società e altresì deve ispirare la condotta dei Consiglieri, dei Dipendenti, dei Collaboratori, nelle relazioni con la



Società

stessa, nonché, all'esterno, con gli Enti istituzionali (istituzioni comunali, provinciali e nazionali), le associazioni di categoria, le associazioni ambientali, e con gli altri *stakeholders*.

Il Codice Etico della SO.GE.R.T. S.p.A. ricomprende:

- a) la sezione programmatica, in cui sono enunciati i principi di deontologia della SO.GE.R.T. S.p.A.;
- b) la sezione nella quale sono indicati gli standard comportamentali comuni, nell'accezione dei diritti e dei doveri a cui sono tenuti tutti coloro che operano con, e per la Società;
- c) la sezione delle procedure di attuazione e di controllo.

2.2.6 Organismo di Vigilanza

Secondo quanto previsto dall'art. 6, comma 1, lettera *b*) del d.lgs. n. 231/2001, il Consiglio di Amministrazione della SO.GE.R.T. S.p.A. nomina l'Organismo di Vigilanza (di seguito anche "OdV"), istituzionalmente preposto all'interno della Società, ma in una posizione di autonomia, alla vigilanza sul funzionamento e sull'osservanza del Modello di organizzazione e gestione, anche al fine di curarne l'aggiornamento.

In particolare, l'OdV è preposto:

1. alla verifica sull'efficacia e sull'adeguatezza del Modello, al fine di comprovarne l'idoneità, rispetto al verificarsi dei reati di cui al Decreto;

2. alla vigilanza sulle condotte dei singoli soggetti dell'Ente, per verificarne la corrispondenza alle procedure e ai protocolli etico - organizzativi di cui al Modello vigente, e l'osservanza delle prescrizioni ivi contenute;
3. all'adozione di ogni provvedimento necessario affinché il Consiglio di Amministrazione ovvero un suo membro a tale scopo delegato (salvo successiva ratifica da parte del Consiglio di Amministrazione), curi il costante aggiornamento del Modello, al fine di assicurarne la tenuta e l'effettività, rispetto ai mutamenti della Società ed alle modifiche normative;
4. all'attuazione delle procedure di controllo previste dal Modello, anche per mezzo di disposizioni interne, di contenuto normativo e/o informativo;
5. a tutte le procedure di verifica e di controllo previste nei protocolli;
6. a garantire, in materia di whistleblowing, l'adeguata formazione dei soggetti che entrano in contatto con l'Ente, la riservatezza dei segnalanti, la loro tutela contro discriminazioni e ritorsioni, la presa in carico delle segnalazioni, la repressione degli illeciti.

Per la nomina dei componenti dell'organo, i requisiti di autonomia, professionalità e continuità d'azione, le relative procedure decisionali e attuative dei compiti dell'Organo, si rinvia al Regolamento dello stesso, che disciplina le modalità di formazione, i processi decisionali e di attuazione delle funzioni dell'organo.

In considerazione della peculiarità delle proprie attribuzioni e dei propri requisiti professionali, l'Organismo di Vigilanza, nello svolgimento dei compiti che gli sono propri, si potrà avvalere

del supporto delle altre funzioni della Società ovvero di Consulenti esterni per il perseguimento dei fini predetti.

Il Consiglio di Amministrazione si impegna ad assegnare, anche in sede di formazione del budget della Società, una dotazione iniziale di risorse finanziarie, anche su proposta dell'Organismo di Vigilanza stesso, il quale ne disporrà nell'esercizio della sua attività.

L'Organismo di Vigilanza è tenuto ad informare il Consiglio di Amministrazione per iscritto, all'inizio di ciascun esercizio, circa il piano di attività predisposto per l'adempimento delle funzioni alle quali è preposto. Riferisce inoltre, immediatamente, le eventuali problematiche applicative e i significativi tratti di discrepanza, rilevati nella verifica dell'applicazione del Modello.

Gli eventuali incontri tra l'Organismo di Vigilanza, l'Organo di Amministrazione ed il Collegio Sindacale dovranno essere documentati per iscritto mediante redazione di appositi verbali.

L'Organismo di Vigilanza svolge una relazione, con cadenza almeno annuale, al Consiglio di Amministrazione in merito alle proprie attività di verifica e, in particolare, in merito all'attuazione del Modello, quindi sulle eventuali violazioni, di cui sia venuto a conoscenza.

L'Organismo di Vigilanza potrà inoltre richiedere agli altri soggetti facenti parte della Società, di riferire in merito al funzionamento del Modello o a situazioni specifiche.

In particolare, l'Organismo di Vigilanza comunica per iscritto i risultati dei propri accertamenti ai Responsabili delle Aree e/o dei processi, in caso di riscontro di comportamenti o azioni non in linea con il Modello, qualora dai controlli scaturissero situazioni a rischio reato.

Quindi, in linea con le procedure della Società, l'OdV acquisisce gli elementi da comunicare

alle strutture preposte, per la valutazione e l'applicazione delle sanzioni disciplinari.

L'Organismo di Vigilanza ha l'obbligo di informare immediatamente per iscritto il Collegio Sindacale qualora la violazione riguardi i Vertici della Società ovvero l'Organo di Amministrazione.

2.2.7 Comunicazione e Formazione

Al fine di garantire l'efficace attuazione del Modello predisposto dalla SO.GE.R.T. S.p.A., è necessario assicurare una corretta conoscenza e divulgazione delle regole di condotta ivi contenute, nei confronti di tutti i soggetti all'interno della Società, dai dirigenti sino ai dipendenti, nonché ai terzi che a qualsiasi titolo intrattengano rapporti con la Società.

La formazione e l'informazione dei soggetti sono assicurati con un diverso grado di approfondimento e con diverse modalità in relazione alla funzione svolta, alle risorse medesime coinvolte nelle attività sensibili e al diverso livello di rischio dell'area considerata.

L'attività di formazione e informazione è affidata all'Organismo di Vigilanza con il supporto dell'Area Personale. Attendere all'attività formativa è obbligatorio, l'inosservanza dell'obbligo è suscettibile di valutazione disciplinare. L'Organismo di Vigilanza effettuerà controlli in merito alla qualità e alla frequenza della formazione.

2.2.7.1 Informativa ai soggetti terzi, esterni alla compagine della Società

Dovranno essere fornite alle istituzioni comunali, provinciali e nazionali, nonché, ai cittadini, ai clienti, ai fornitori, alle associazioni di categoria, alle associazioni ambientali, ecc. apposite

informative sulle politiche e le procedure adottate sulla base del Modello, mediante idonea diffusione.

Ai fini di un'adeguata attività informativa, i soggetti della Società competenti, in stretta cooperazione con l'Organismo di Vigilanza, provvederanno a curare la diffusione del contenuto del Modello ai predetti soggetti mediante pubblicazione della parte generale del Modello sul sito internet della SO.GE.R.T. S.p.A.

I soggetti destinatari possono essere invitati a rilasciare, a cura della funzione interessata, una dichiarazione sottoscritta ove si attesti la conoscenza del contenuto del Codice Etico e del Modello (Parte Generale e Parte Speciale) della Società, nonché l'impegno ad osservarne le prescrizioni, e a non tenere condotte che possano esporre la Società alla responsabilità da reato di cui al D.lgs. n. 231/01.

Nell'ambito dell'attività svolta da SO.GE.R.T. S.p.A. con riferimento alla riscossione, liquidazione, accertamento, comprese le fasi coattive, delle entrate tributarie ed extra tributarie, incluse le sanzioni a qualsiasi titolo emesse, nonché servizi integrativi ed ausiliari alla attività di riscossione stessa su tutto il territorio italiano, per garantire il corretto adempimento di quanto previsto dal bando di gara aggiudicato presso ciascun ente locale, la società potrà sottoscrivere contratti d'opera con società terze per la fornitura di beni e/o servizi.

Innanzitutto la SO.GE.R.T. S.p.A., consapevole che (in linea generale) i bandi di gara non consentono alla ditta aggiudicatrice di subappaltare i servizi previsti, si impegna a sottoscrivere con società terze solo ed esclusivamente contratti così come previsti dall'art. 2222 c.c.

Inoltre, proprio nell'ottica di una corretta gestione aziendale e del rispetto dei principi etici, la SO.GE.R.T. S.p.A. ritiene di dover disciplinare i rapporti con queste società terze nell'ambito del modello organizzativo.

Pertanto, qualora la società con cui si andrà a sottoscrivere un contratto di prestazione d'opera sia dotata di un Modello Organizzativo ex D.lgs. 231/01 nonché di un Organismo di Vigilanza, sarà opportuno che vi sia un flusso di informazioni tra i due organi di controllo con specifico riferimento all'ambito di attività svolto in virtù dell'accordo.

Se invece la società terza non si sia dotata di un Modello Organizzativo ex D.lgs. 231/01, sarà necessario che la SO.GE.R.T. S.p.A. individui un proprio dipendente che svolga funzioni di monitoraggio sul rispetto dei principi posti alla base del suo Modello Organizzativo nello svolgimento delle attività previste dal contratto.

Entrambe queste previsioni dovranno essere parte integrante del contratto di prestazione d'opera che la SO.GE.R.T. S.p.A. andrà a sottoscrivere.

2.2.7.2 I flussi informativi che coinvolgono l'Organismo di Vigilanza

Al fine di agevolare l'attività di vigilanza sull'efficacia del Modello a cui l'OdV, è istituzionalmente previsto che, in presenza di eventuali situazioni dove può essere possibile il verificarsi dei reati di cui al d.lgs. n. 231/2001, debbano essere obbligatoriamente trasmesse all'Organismo di Vigilanza, da parte dei soggetti interessati, tutte le informazioni utili a tale scopo, tra cui a titolo esemplificativo, quelle relative:

- alle risultanze delle procedure di verifica e di controllo, dalle quali emergano criticità, in sede di attuazione del Modello;
- alle anomalie e alle atipicità riscontrate dalle funzioni della Società;
- ai provvedimenti e/o alle informative della polizia giudiziaria o di qualsiasi altra autorità, da cui si evinca l'esistenza di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
- alle comunicazioni interne ed esterne riguardanti qualsiasi circostanza, che possa essere connessa ai fatti da reato di cui al Decreto (cfr. provvedimenti disciplinari nei confronti di Dipendenti);
- ad eventuali commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al d.lgs. n. 231/2001;
- ai procedimenti disciplinari svolti, alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati alla commissione di taluno dei reati di cui al decreto;
- alle notizie relative a cambiamenti dell'assetto organizzativo della Società;
- a modifiche inerenti il sistema delle deleghe all'interno della Società;
- alla realizzazione di operazioni significative o atipiche, nel cui contesto possono annidarsi

ipotesi di rischio – reato;

- a mutamenti nelle situazioni di rischio o potenzialmente a rischio di taluni dei reati di cui al

Decreto.

Per quanto attiene invece, alle eventuali comunicazioni del Collegio Sindacale, o comunque della funzione Amministrazione, Finanza e Controllo, rispetto a carenze nel sistema dei

controlli interni, fatti censurabili, osservazioni sul bilancio della Società, queste devono essere portate direttamente a conoscenza, dell'Organismo di Vigilanza.

All'Organismo di Vigilanza devono essere altresì portate a conoscenza:

- le informazioni contenute nelle comunicazioni sociali;
- i verbali delle riunioni del Consiglio di Amministrazione, del Collegio Sindacale;
- le attività intrattenute con la Pubblica Amministrazione (in particolare con le istituzioni comunali e provinciali);
- le eventuali erogazioni pubbliche di cui la Società dovesse essere beneficiaria;
- le comunicazioni delle Autorità amministrative o fiscali, relative alle attività di verifica svolte sul bilancio, sulle comunicazioni tributarie, e agli esiti delle ispezioni effettuate presso la Società;
- qualsiasi altra informazione, in qualunque modo acquisita, relativa alla commissione dei reati previsti dal Decreto o a comportamenti in violazione delle prescrizioni del Modello.

Dovranno essere altresì assicurate le opportune procedure di comunicazione, tali da consentire un agevole e tempestivo flusso informativo verso l'Organismo di Vigilanza, da parte dei soggetti che vengano in possesso delle notizie e delle circostanze sopra indicate, o relative alla commissione di reati o situazioni non conformi con le prescrizioni del Modello o del Codice Etico.

L'Organismo di Vigilanza verifica e assicura che le procedure di segnalazione delle suddette

circostanze avvengano nel pieno anonimato, a tutela della riservatezza dei soggetti informatori, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

I report e la documentazione rilevante ai fini “231” dovranno essere conservati agli atti, da parte delle Direzioni/Funzioni interessate e dell’Organismo di Vigilanza, per un periodo non inferiore a 5 anni.

L’Organismo di Vigilanza valuterà le segnalazioni ricevute, riferendo circa l’intero iter di verifica, nelle comunicazioni periodiche che è tenuto ad effettuare.

In ogni caso l’Organismo di Vigilanza ha accesso presso tutte le funzioni della Società e, dunque, presso tutto il personale della stessa, – senza necessità di alcuna autorizzazione preventiva – al fine di ottenere, ricevere e raccogliere le suddette informazioni e in generale ogni informazione o dato utile per lo svolgimento della propria attività.

2.2.8 Sistema disciplinare

L’implementazione di un efficace Sistema Disciplinare, quale parte integrante del Modello, idoneo a sanzionarne la mancata attuazione o la violazione delle prescrizioni in esso indicate, è condizione essenziale per garantire l’effettività del Modello stesso, secondo quanto prevede l’art. 6, comma 2, lettera e) del Decreto.

L’applicazione delle sanzioni disciplinari costituisce la risposta afflittiva e general preventiva nei confronti del trasgressore da parte della *Governance* della Società.

L’accertamento della responsabilità dell’autore delle violazioni avviene secondo modalità opportune ad assicurargli il contraddittorio, nel procedimento di verifica della responsabilità e di contestazione della sanzione.

Il sistema disciplinare adottato costituisce l'esito applicativo delle eventuali criticità riscontrate nell'esercizio delle funzioni di vigilanza e monitoraggio da parte degli organi interni ed esterni alla Società.

Le sanzioni possono essere irrogate quando, in riferimento alla violazione delle regole comportamentali disposte dal modello e/o dal Codice etico, sia stata accertata la colpevolezza del soggetto responsabile, indipendentemente dalla verifica della stessa nelle opportune sedi giurisdizionali, attraverso la procedura di accertamento delle predette condotte che esso prevede.

In particolare, ai fini dell'applicazione delle rispettive sanzioni, sono rilevanti le condotte di violazione e di elusione delle regole comportamentali disposte dal modello e/o dal Codice Etico, nonché le volontarie elusioni delle stesse e le applicazioni colpose imperfette.

Il Sistema disciplinare adottato della Società prevede, altresì, un'apposita procedura di irrogazione delle sanzioni applicabili, individuando il soggetto preposto alla loro irrogazione e in generale a vigilare sulla osservanza, l'applicazione e l'aggiornamento del Sistema Disciplinare, anche in riferimento agli organi dirigenziali della Società.

3. Il Modello di *Governance* ed il Sistema Organizzativo

3.1 Il Modello di *Governance* della SO.GE.R.T. S.p.A.

Il sistema di *Corporate Governance* della SO.GE.R.T. S.p.A. risulta, attualmente composto dai seguenti organi:

Assemblea dei soci ordinaria

Spetta all'assemblea ordinaria dei soci la formulazione degli indirizzi e la programmazione sulla gestione della società. L'assemblea ordinaria dei soci infatti, delibera nelle materie previste dalla legge, ed in particolare:

1. approva il bilancio;
2. nomina gli Amministratori, il Presidente del Consiglio d'Amministrazione, i Sindaci, il Presidente del Collegio Sindacale ed il soggetto al quale è demandato il controllo contabile, determinandone contemporaneamente il compenso;
3. delibera sulla responsabilità degli amministratori e dei Sindaci;
4. delibera su altri oggetti sottoposti al suo esame dal Consiglio d'Amministrazione;
5. delibera su ogni altra materia alla stessa riservata dalla legge.

Assemblee speciali

Ai sensi dell'art. 2365, comma 1, del Codice Civile, l'assemblea straordinaria delibera sulle modificazioni dello Statuto, sulla nomina, sulla sostituzione e sui poteri dei liquidatori e su ogni altra materia espressamente attribuita dalla legge alla sua competenza.

Consiglio di Amministrazione

Il Consiglio di Amministrazione è composto di 3 membri, un Presidente, un consigliere, e un Consigliere Delegato. L'organo amministrativo, nel rispetto degli indirizzi di assemblea, è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società e può compiere tutti gli atti che ritenga necessari ed opportuni per il conseguimento dell'oggetto sociale, ad esclusione di quelli riservati all'Assemblea dalla legge e dallo Statuto.

All'Organo amministrativo spetta in via non esclusiva la competenza per adottare le deliberazioni concernenti la fusione nel caso previsto dall'art. 2505bis, l'istituzione o la soppressione di sedi secondarie, l'indicazione di quali tra gli amministratori hanno la rappresentanza della società, la riduzione del capitale in caso di recesso del socio, gli adeguamenti dello statuto a disposizioni normative, il trasferimento della sede sociale nell'ambito del territorio italiano.

Il Consiglio d'Amministrazione può nominare direttori e procuratori delegando agli stessi in tutto o in parte le proprie attribuzioni promuovere azioni giudiziarie, in ogni sede e grado di giurisdizione, nominare avvocati e procuratori anche in sede di cassazione e nominare mandatarî ad negozia.

Presidente CdA

Il Presidente del Consiglio d'Amministrazione è eletto dai membri del Consiglio d'Amministrazione ed allo stesso compete la rappresentanza legale della società di fronte ai terzi ed in giudizio.

Compete altresì al Presidente convocare il Consiglio d'Amministrazione e dirigerne i lavori.

Collegio Sindacale

Il Collegio Sindacale vigila sull'osservanza della legge e dello statuto sociale, sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo amministrativo e contabile adottato dalla società e sul suo concreto funzionamento; è composto da tre sindaci effettivi e due supplenti nominati dall'Assemblea. Con il medesimo atto l'Assemblea nomina, fra i tre sindaci, il Presidente.

Il controllo contabile è esercitato dal Collegio Sindacale integralmente costituito da revisori contabili iscritti nel Registro istituito presso il Ministero della Giustizia.

I sindaci durano in carica tre esercizi e scadono a data dell'assemblea convocata per l'approvazione del bilancio relativo al terzo esercizio della carica.

3.2 Struttura Organizzativa della SO.GE.R.T. S.p.A.

La struttura organizzativa della Società è orientata a garantire, la separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo. A tale proposito, SO.GE.R.T. S.p.A., si è dotata di strumenti organizzativi, anche se parzialmente basati su usi e consuetudini, improntati ai principi generali di:

- conoscibilità dei processi e di coloro che vi operano all'interno della Società;
- chiara e formale delimitazione dei ruoli.

Conseguentemente, le procedure e le prassi attualmente in essere sono improntate ai seguenti criteri:

- la separazione di funzioni, all'interno di ciascun processo, per cui l'impulso decisionale, l'effettuazione, la conclusione ed il controllo di ogni operazione devono essere attribuiti a soggetti diversi. Il principio della separazione delle funzioni consente la chiara attribuzione delle responsabilità e dei poteri di rappresentanza, nel rispetto delle linee gerarchiche;
- la documentazione di ciascun passaggio rilevante del processo: il principio assume un ruolo fondamentale nel caso di transazioni e operazioni economiche, al fine di poter procedere, in ogni momento, all'effettuazione di controlli che chiariscano le caratteristiche e le motivazioni dell'operazione, ed individuino chi ha autorizzato, effettuato, registrato e verificato l'operazione stessa;
- adeguati livelli di formalizzazione ed informazione;
- la costituzione di un sistema chiaro di deleghe e procure.

La valutazione preliminare dell'assetto organizzativo della Società è stata effettuata mediante l'analisi delle informazioni ottenute tramite specifiche interviste effettuate con il personale apicale della società.

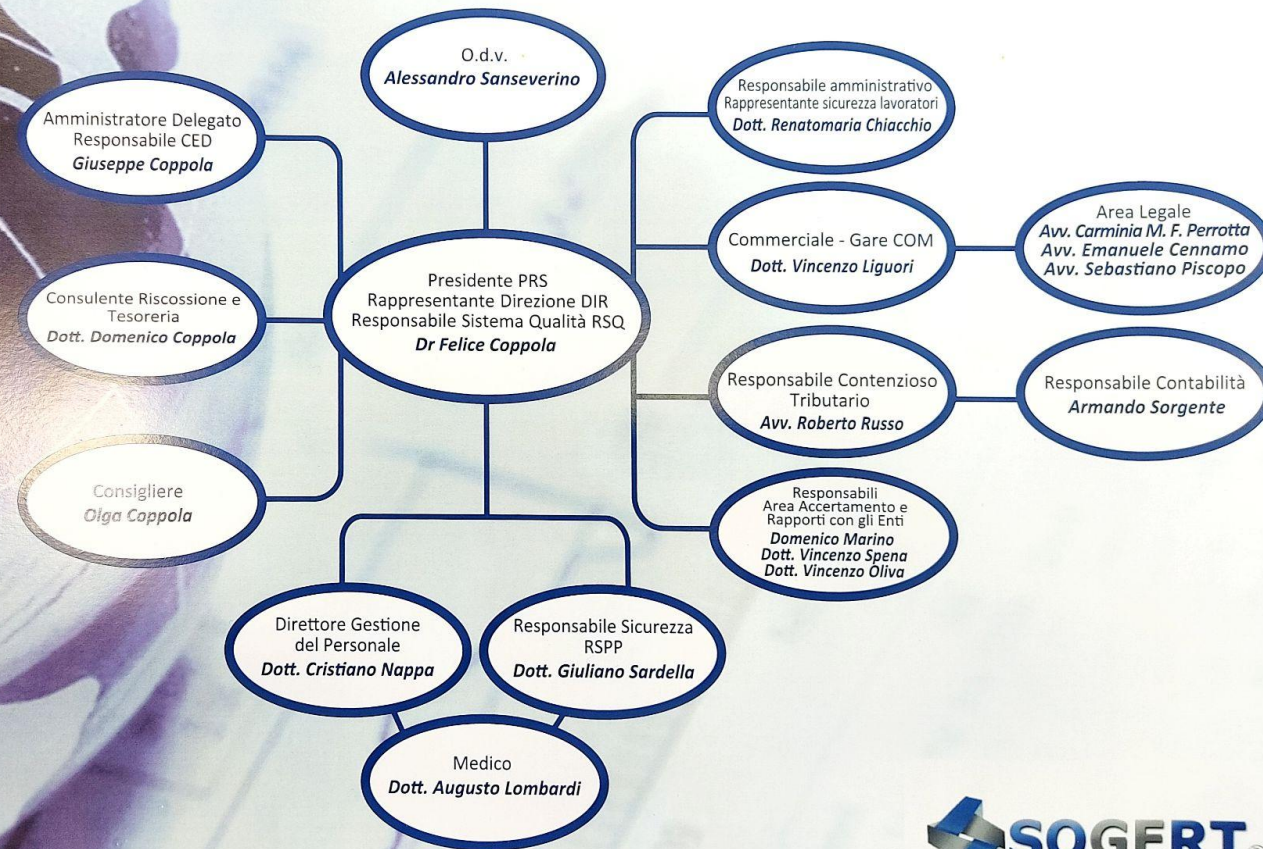
In particolare, la valutazione dell'assetto organizzativo della Società è stata basata sull'Organigramma aziendale attualmente vigente.

La struttura organizzativa, retta e coordinata dal Presidente del Consiglio di Amministrazione, con il supporto dell'Amministratore Delegato, le cui attribuzioni sono definite rispettivamente dallo Statuto e dal Consiglio d'Amministrazione, è stata descritta in un organigramma suddiviso in 9 Aree, ciascuna delle quali è retta da un responsabile:

- Direzione Generale;

- Area Legale e Contenzioso Tributario;
- Area Amministrativa;
- Area Personale;
- Area Commerciale e Gare;
- Area Accertamento e Riscossione;
- Area Gestione Tesoreria.
- Area Qualità;
- Area Sicurezza.

ORGANIGRAMMA AZIENDALE



3.3 Descrizione delle deleghe e individuazione dei soggetti ‘apicali’ e ‘subalterni’

Il livello di autonomia, il potere di rappresentanza, i poteri di firma ed i limiti di spesa assegnati ai titolari di deleghe e procure all’interno dell’Ente devono essere individuati e fissati in modo coerente con il livello gerarchico del destinatario della delega o della procura nei limiti di quanto strettamente necessario all’espletamento dei compiti e delle mansioni oggetto di delega.

Tutti coloro che intrattengono rapporti con la Pubblica Amministrazione e con i terzi in genere, per conto della SO.GE.R.T. S.p.A., devono essere dotati di delega formale.

Le deleghe devono associare il potere di gestione alla relativa responsabilità e ad una posizione adeguata nell’organigramma; esse devono essere aggiornate in conseguenza dei mutamenti organizzativi.

Ciascuna delega deve definire in modo specifico ed inequivocabile i poteri del delegato ed il soggetto (organo ed individuo) cui il delegato riporta gerarchicamente; il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

Nell’ambito dell’organigramma della SO.GE.R.T. S.p.A., i *soggetti apicali* individuati risultano i seguenti:

- Presidente del Consiglio d’Amministrazione;
- Amministratore Delegato;
- Direttore Generale;
- Responsabile Area Legale e Contenzioso Tributario;
- Responsabile Area Amministrativa;
- Direttore Gestione del Personale;

- Responsabile Area Commerciale e Gare;
- Responsabile dell'Accertamento e della Riscossione;
- Responsabile della Tesoreria;
- Responsabile del Sistema Qualità;
- Responsabile della Sicurezza.

4. Identificazione delle aree della Società a rischio reato (*Risk Assessment*) e verifica dei sistemi di controllo esistenti (*Gap Analysis*)

a. *Risk Assessment e Gap Analysis*

Il *management* della Società, costituito dai Responsabili delle Direzioni sopra richiamate, nonché alcuni loro Collaboratori, sono stati coinvolti, sulla scorta delle informazioni acquisite, nell'analisi della struttura organizzativa, dalla cui elaborazione sono state identificate le macro-aree a rischio, nell'ambito delle quali è possibile ipotizzare l'eventuale commissione dei reati di cui al D.lgs. n. 231/2001.

L'analisi delle situazioni di rischio esistenti, sono state condotte considerando l'assetto organizzativo e procedurale della SO.GE.R.T. S.p.A., alla data di redazione del Modello; in particolare le macro-aree ed i processi a rischio, sono stati analizzati nel dettaglio, in riferimento al fattore di rischio potenziale, dato ogni singolo reato presupposto della responsabilità della Società.

Da ciò, si è potuto evincere che le fattispecie di reato, di cui al D.lgs. n. 231/2001, rilevanti per la SO.GE.R.T. S.p.A. sono le seguenti:

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25);**
- **Salute e sicurezza sui luoghi di lavoro (art. 25^{septies})**
- **Delitti informatici e trattamento illecito di dati (art. 24 *bis*);**
- **Reati tributari (art. 25-*quinqüesdecies*).**

Le principali macro-aree di rischio individuate sono le seguenti:

- Gestione dei flussi informativi interni;
- Risk management;
- Rapporti con la Pubblica Amministrazione;
- Gestione delle risorse umane;
- Assegnazione incarichi;
- Organo amministrativo.

Individuate le aree a rischio reato e, all'interno delle stesse, le attività e le funzioni della Società maggiormente sensibili, sono state evidenziate le possibili modalità di realizzazione dei reati presupposto della responsabilità della Società stessa, unitamente, per le aree oggetto di analisi, all'esplicitazione dei più significativi fattori di rischio che possono favorire il verificarsi delle modalità di realizzazione dei reati, nonché dei controlli tesi a mitigare i suddetti fattori di rischio (*cd. Risk Assessment*).

In particolare, l'attività di individuazione e censimento delle aree/processi/sotto-processi sensibili si è articolata in una serie di fasi successive. La prima è quella di c.d. *Process Assessment*, ossia di analisi delle attività e dei processi delle singole aree della Società, condotta mediante l'esame dei risultati delle interviste effettuate, in maniera guidata, ai

Responsabili delle funzioni dell'Ente (c.d. “soggetti apicali”) identificati tramite l'analisi dell'assetto organizzativo. Le interviste puntano ad evidenziare, facendo specifico

riferimento alla posizione assegnata ed alle mansioni svolte, sia le eventuali lacune e/o carenze organizzative che il soggetto percepisca nell'ambito delle proprie attività, sia le relazioni che intrattiene con colleghi in posizioni omogenee, nonché con la Presidenza della società.

La fase successiva è quella di c.d. *Risk Assessment*, ossia di verifica e abbinamento di ciascuna macro-categoria di reati presupposto (e dei singoli reati tipici in essa ricompresi) allo specifico processo gestito dalla singola Area dell'Ente.

Ai fini della elaborazione di un efficace ed effettivo *Compliance program* idoneo all'ottenimento del beneficio giudiziale dell'esimente da responsabilità della Società, sono stati presi in considerazione i soli comportamenti attivi od omissivi idonei alla realizzazione delle specifiche fattispecie sostanzianti in un reato tipico ex D.lgs. 231/01; alcuni comportamenti prodromici o strumentali, accessori o eventuali non idonei ex se alla consumazione (o al tentativo) del reato tipico sono stati comunque valutati, sebbene non assumano il rilievo di specifico rischio-reato.

I singoli reati sono stati censiti e mappati con riguardo alle funzioni espletate dalle specifiche Aree della Società ed, in esse, con riguardo al peculiare macro-processo o singolo processo individuato. Tale rischiosità risulta valutata con riferimento temporale alla data di effettuazione dell'identificazione delle aree a rischio.

In particolare si è ritenuto opportuno prendere in considerazione, nell'ambito del Modello stesso, i rischi relativi alla commissione di tutte le fattispecie di reato richiamate dal Legislatore, alla data di effettuazione dell'identificazione delle aree a rischio.

Tale decisione è stata dettata essenzialmente da due ragioni:

- da un lato, si ritiene non possano esistere settori di attività della Società in cui il

rischio di commissione di un qualsiasi reato richiamato dal Provvedimento possa essere astrattamente ritenuto inesistente, sebbene la sua consumazione nella realtà della Società sembri difficilmente ipotizzabile;

- dall'altro, la Società è convinta dell'opportunità di esprimere principi comportamentali volti a stigmatizzare tutte le condotte criminose, anche virtualmente realizzabili nel proprio ambito imprenditoriale, dando così prova tangibile della riprovazione nei confronti di chiunque dovesse porre in essere simili attività.

L'enunciazione di regole di condotta e il rinvio all'osservanza del Codice Etico che, giova ricordarlo, è da ritenere a ogni effetto parte integrante del Modello, sono finalizzati a diffondere l'etica d'impresa di cui la SO.GE.R.T. S.p.A. è portatrice, anche alla luce delle considerazioni precedentemente svolte.

Con riferimento alla verifica dei sistemi di controllo esistenti, in sede di mappatura delle Aree della Società e di censimento dei rischi-reato concretamente rilevati, per ciascuna *macro area sensibile*, è stata verificata l'esistenza e la funzionalità, in chiave preventiva ex D.lgs. 231/2001, di eventuali sistemi di *Risk control* interno già vigenti all'interno dell'Ente, sebbene preordinati a diversa funzionalità e finalità (c.d. *Gap Analysis*).

Gli *output* risultanti dalle attività di identificazione delle aree a rischio e dalla *Gap Analysis* si articolano in una serie di documenti, costituenti parte integrante del Modello:

- A. **MATRICI ANALISI PROCESSI DELLA SOCIETA'** (Allegato n. 1):
evidenziano visivamente i singoli rischi-reato rilevati (caselle di colore rosso), frutto dell'abbinamento di ciascun reato tipico facente parte della medesima macro-

categoria alle singole carenze organizzative individuate nell'ambito dei macro

processi gestiti nella specifica Area della Società interessata per i quali si ritiene sussista una concreta potenzialità commissiva.

B. MAPPA DELLE MACRO AREE SENSIBILI / CRITICITA' DEL SISTEMA

ORGANIZZATIVO E DI CONTROLLO ESISTENTE: di seguito sono riportati

i risultati della *Gap Analysis* per ciascuna Area:

Rapporti con la Pubblica Amministrazione

AREA	MACRO AREA SENSIBILE	CRITICITA' DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO
Alta direzione	Gestione rapporti con gli enti Pubblici	Carenza di una procedura formalizzata che identifichi chiaramente i soggetti che entrano in contatto con i vari Enti pubblici/C omuni ecc. e ne definisca compiti e responsabilità
Alta direzione / Amministrazione / Ufficio legale / Sedi periferiche / Personale	Rapporti con Organi Ispettivi	Sussiste il rischio di commissione dei reati di corruzione e concussione in quanto la Società o soggetti ad essa appartenenti, al fine di ottenere un trattamento preferenziale in sede di ispezione, potrebbero intrattenere rapporti confidenziali con pubblici dipendenti erogando loro denaro o altre utilità. Il rischio può concretizzarsi, ad esempio, in relazione a verifiche in ambito fiscale, previdenziale, della sicurezza sul lavoro, sanitario, ecc.
Alta direzione	Assegnazione e gestione incarichi di consulenza	Sussiste il rischio di commissione di condotte corruttive nel processo di assegnazione di incarichi o consulenze al fine di veicolare denaro o altre utilità verso soggetti pubblici o soggetti in grado di influenzare le scelte di soggetti pubblici, con il fine unico o prevalente di apportare vantaggi alla Società.
Alta direzione / Uff. Personale	Ricerca, selezione e assunzione personale	Sussiste il rischio di commissione di condotte corruttive mediante l'assunzione di personale avente rapporti diretti o indiretti con soggetti appartenenti alla P.A. ovvero con ex esponenti della PA
Alta direzione / Uff. Personale	Incentivi al personale	Sussiste il rischio di commissione di condotte corruttive mediante la promozione e l'incentivazione di personale avente rapporti diretti o indiretti con soggetti appartenenti alla P.A. ovvero con ex esponenti della PA
Alta direzione / Amministrazione	Registrazione e pagamento fatture passive	Sussiste il rischio di commissione di reati societari connessi a false scritture contabili e di creazione di fondi di denaro occulti mediante operazioni di fatturazione/pagamento per forniture inesistenti; ovvero, mediante l'acquisto di beni o servizi presso fornitori che abbiano rapporti preferenziali con soggetti appartenenti alla P.A. è possibile ottenere, indirettamente, vantaggi per la società.
Alta direzione / Amministrazione	Gestione rimborsi spese	Sussiste il rischio di creazione di fondi neri per fini corruttivi attraverso registrazioni di rimborsi spese relativi a missioni e trasferte per importi superiori a quello reale o a fronte di missioni inesistenti

Salute e Sicurezza sul lavoro

AREA	MACRO AREA SENSIBILE	CRITICITA' DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO
Alta Direzione	Gestione salute e sicurezza sui luoghi di lavoro	Corretta attuazione delle misure di prevenzione in base alla normativa vigente

Delitti informatici e trattamento illecito di dati

AREA	MACRO AREA SENSIBILE	CRITICITA' DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO
Alta direzione / Amministrazione / Ufficio legale / Sedi periferiche / Personale	Utilizzo rete	Rigide restrizioni di accesso alla rete ed ai software aziendali
	Inserimento dati	Assegnazione, ad ogni singolo dipendente, di un account personale per accedere alle postazioni
		Cronologia delle operazioni effettuate dai singoli account per poter risalire al dipendente che ha effettuato operazioni sospette

Reati Tributari:

Area	Macroarea sensibile	Criticità del sistema organizzativo e di controllo
Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità	- Rapporti con controparti; - Approvvigionamento di beni e servizi; - Pagamenti.	Sussiste il rischio di commissione dei reati tributari, ad esempio mediante fatturazioni oggettivamente ovvero soggettivamente inesistenti o recanti corrispettivi o importi iva differenti rispetto a quelli reali. Inoltre, può accadere che i pagamenti effettuati siano di importo inferiore rispetto a quanto dichiarato o certificato, come nel caso della corresponsione degli stipendi.
	- Contabilità; - Fatture e altri documenti contabili; - Presentazione delle dichiarazioni; - Rapporti con eventuali consulenti esterni in materia fiscale.	Sussiste il rischio di commissione dei reati tributari, ad esempio per il mezzo dell'utilizzo di fatture o altri documenti per operazioni inesistenti, ovvero per l'occultamento o la distruzione della documentazione contabile.
	- Operazioni straordinarie; - Emissione di assegni.	Sussiste il rischio di commissione dei reati tributari, ad esempio mediante atti fraudolenti su beni aziendali, al fine di sottrarli ad una probabile procedura esecutiva.
	- Formazione ed informazione del personale	La commissione dei reati tributari potrebbe essere agevolata dalla mancata conoscenza del personale.

5. Comunicazione e Formazione

5.1 Diffusione del Modello

SO.GE.R.T. S.p.A. promuove la più ampia divulgazione, all'interno e all'esterno della struttura, dei principi e delle previsioni contenuti nel Modello e nei Protocolli ad esso connessi.

Il Modello è comunicato formalmente a tutti i soggetti apicali (inclusi gli Consiglieri, i Sindaci ed i Revisori) ed al Personale della Società mediante consegna di copia integrale, anche su supporto informatico o in via telematica, nonché mediante pubblicazione sulla rete intranet della Società ed affissione in luogo accessibile a tutti. Per i soggetti esterni alla Società destinatari del Modello e del Codice Etico, secondo quanto previsto dal precedente paragrafo 2.2.4 sono previste apposite forme di comunicazione del Modello e del Codice Etico. I contratti che regolano i rapporti con tali soggetti, devono prevedere chiare responsabilità in merito al rispetto delle politiche della Società e in particolare al suo Codice Etico e del presente Modello.

Della eseguita consegna e dell'impegno da parte dei Destinatari al rispetto delle regole ivi previste viene conservata traccia documentale agli atti dell'OdV.

Per i Terzi Destinatari tenuti al rispetto del Modello, lo stesso sarà reso disponibile nelle forme che la SO.GE.R.T. S.p.A. riterrà più opportune.

Sotto tale ultimo aspetto, al fine di formalizzare l'impegno al rispetto dei principi del Modello nonché dei Protocolli ad esso connessi da parte di Terzi Destinatari, è previsto l'inserimento nel contratto di riferimento di una apposita clausola, ovvero, per i contratti già in essere, la sottoscrizione di una specifica pattuizione integrativa, in tal senso.

L'OdV promuove, anche mediante la predisposizione di appositi piani, e monitora tutte le ulteriori attività di informazione che dovesse ritenere necessarie o opportune.

Il coinvolgimento dei soggetti interessati è assicurato anche mediante la loro consultazione preventiva in occasione di apposite riunioni periodiche.

5.2 Formazione e addestramento sul Modello e sui Protocolli etico-organizzativi

In aggiunta alle attività connesse alla Informazione dei Destinatari, l'OdV ha il compito di curarne la periodica e costante Formazione, ovvero di promuovere e monitorare l'implementazione, da parte della Società, delle iniziative volte a favorire una conoscenza ed una consapevolezza adeguate del Modello e dei Protocolli ad esso connessi, al fine di incrementare la cultura etica all'interno della Società stessa.

In particolare, è previsto che i principi del Modello, ed in particolare quelli del Codice Etico, che ne è parte integrante, siano illustrati ai destinatari, attraverso apposite attività formative (ad es. corsi, seminari, questionari, ecc.), a cui è posto obbligo di partecipazione e le cui modalità di esecuzione sono pianificate dall'OdV mediante predisposizione di specifici Piani implementati dalla società.

I corsi e le altre iniziative di formazione sui principi del Modello sono, peraltro, differenziati in base al ruolo ed alla responsabilità delle risorse interessate, ovvero mediante la previsione di una formazione più intensa e caratterizzata da un più elevato grado di approfondimento per i soggetti qualificabili come “apicali” alla stregua del Decreto, nonché per quelli operanti nelle aree qualificabili come “a rischio” ai sensi del Modello.

La Società promuove, inoltre, la formazione e l'addestramento dei Destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, al fine di assicurare un'adeguata consapevolezza circa l'importanza sia della conformità delle azioni rispetto al Modello, sia delle possibili conseguenze connesse a violazioni dello stesso. A tali fini, è definito, documentato, implementato, monitorato ed aggiornato, da parte della Società, un programma di formazione ed addestramento periodici dei Destinatari del Modello.

In particolare, si prevede che la formazione e l'addestramento siano differenziati in base al posto di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro, di nuove tecnologie, di nuove sostanze e preparati pericolosi.

PARTE SPECIALE

	Protocollo Etico – Organizzativo	PRO.1
	Gestione dei rapporti con la Pubblica Amministrazione	

INDICE

1. SCOPO	2
2. AMBITO DI APPLICAZIONE	3
3. REATI DI CUI AGLI ARTT 24 E 25 DEL D.LGS. N. 231/2001	3
4. REATI DI CUI ALLA L. 190/2012	4
5. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITÀ SENSIBILI	10
6. PRINCIPI COMPORTAMENTALI DA ADOTTARE	11
7. RESPONSABILITÀ E REPORTISTICA ALL'ORGANISMO DI VIGILANZA	14

INDICE DELLE REVISIONI				
REV	DATA	OGGETTO	REDATTO *** da ...	APPROVATO da ...

1. SCOPO

La presente norma comportamentale ha lo scopo di illustrare i principi che devono essere seguiti nella gestione degli adempimenti verso la Pubblica Amministrazione e nella predisposizione della relativa documentazione.

Preliminare all'analisi dei reati contro la Pubblica Amministrazione, richiamati dagli artt. 24 e 25 del D.lgs. n. 231/2001 (di seguito, anche, 'Decreto'), è la delimitazione delle nozioni di **Pubblica Amministrazione** (di seguito "**P.A.**"), di **Pubblico Ufficiale** (di seguito "**PU**") e di **Incaricato di Pubblico Servizio** (di seguito "**IPS**").

Per **P.A.** si intende, in estrema sintesi, l'insieme di enti e soggetti pubblici (Stato, ministeri, regioni, province, comuni, etc.) e talora privati (ad es., concessionari, amministrazioni aggiudicatrici, S.p.A. miste, ecc.) e tutte le altre figure che svolgono in qualche modo la funzione pubblica, nell'interesse della collettività e quindi nell'interesse pubblico. Oggetto della tutela penale nei reati che rilevano in questa sede è il regolare funzionamento nonché il prestigio degli Enti Pubblici ed, in generale, quel 'buon andamento' dell'Amministrazione di cui all'art. 97 della Costituzione, ovvero, nel caso dei reati di truffa, il patrimonio pubblico.

La nozione di **P.U.** è fornita direttamente dal legislatore, all'art. 357 del cod. pen., il quale indica il "pubblico ufficiale" in *"chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa"*, specificandosi che *"è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica Amministrazione e dal suo svolgersi per mezzo dei poteri autoritativi e certificativi"*.

Diversamente, l'art. 358 del cod. pen. riconosce la qualifica di "incaricato di un pubblico servizio" a tutti *"coloro i quali, a qualunque titolo, prestano un pubblico servizio"*, intendendosi per tale *"un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale"*.

È, pertanto, un IPS colui il quale svolge una 'pubblica attività', non riconducibile ad alcuno dei 'poteri' sopra rammentati e non concernente semplici mansioni d'ordine e/o la prestazione di opera meramente materiale ed, in quanto tali, prive di alcun apporto intellettuale e discrezionale. Esempi di IPS sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati.

2. AMBITO DI APPLICAZIONE

La norma si applica a tutte le Funzioni aziendali che, nell'espletamento delle attività di propria competenza, si trovino a dover gestire rapporti con la Pubblica Amministrazione in merito, in via esemplificativa, a:

- partecipazione a pubbliche gare;
- predisposizione di certificati e dichiarazioni;
- richiesta di contributi e finanziamenti;
- ottenimento di certificati e concessioni;
- stipulazione di convenzioni, contratti, accordi e protocolli d'intesa;
- comunicazione di dati societari /aziendali di qualsiasi natura.

3. REATI DI CUI AGLI ARTT. 24 E 25 DEL D.LGS. N. 231/2001

Si riporta di seguito una sintetica descrizione dei reati richiamati negli artt. 24 e 25 del Decreto, nonché una breve esposizione delle possibili modalità di attuazione dei reati, fermo restando che, ai sensi dell'art. 26 del Decreto, la Società potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

Malversazione in danno dello Stato o di altro Ente Pubblico (art. 316bis c.p.)

Il reato si configura qualora, dopo aver ricevuto da parte dello Stato italiano, di altro Ente Pubblico o della Unione Europea, finanziamenti, sovvenzioni o contributi destinati alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non si proceda all'utilizzo o alla destinazione delle somme ottenute per gli scopi cui erano originariamente destinate.

In concreto, occorre che le attribuzioni in denaro siano state distratte, anche parzialmente, senza che rilevi che l'attività programmata sia stata comunque realizzata.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui, a seguito della percezione di un finanziamento pubblico erogato per determinati fini, si ometta di destinare le somme percepite per tali finalità.

Indebita percezione di contributi, finanziamenti o altre erogazioni in danno dello Stato o di un Ente Pubblico (316ter c.p.)

Il reato si configura allorché, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi ovvero mediante l'omissione di informazioni dovute, si ottengano, pur senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri Enti Pubblici o dall'Unione Europea.

In questa fattispecie, diversamente da quanto accade nel reato di malversazione in danno dello Stato o di altro Ente Pubblico (art. 316bis c.p.), non ha alcuna rilevanza l'uso che viene fatto delle erogazioni, perfezionandosi il reato con il solo ottenimento degli indebiti finanziamenti.

Tale ipotesi di reato assume natura residuale rispetto alla più grave fattispecie di truffa in danno dello Stato (ex art. 640, II comma, n. 1 c.p.), per la cui sussistenza è necessaria l'induzione in errore mediante artifici o raggiri.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui il finanziamento venga concesso a seguito dell'utilizzazione di documenti falsi.

Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, II comma, n. 1, c.p.)

Il reato si configura qualora, utilizzando artifici o raggiri ed in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro Ente Pubblico o dell'Unione Europea.

Per "artificio" o "raggiro" si intende la simulazione o dissimulazione della realtà, atta ad indurre in errore una persona per effetto della percezione di una falsa apparenza. Il silenzio può integrare la condotta della truffa se attuata in presenza di un obbligo giuridico di comunicazione, anche di carattere extrapenale.

L'atto di disposizione del soggetto indotto in errore può comprendere ogni comportamento dotato di una efficacia in fatto; tale può essere considerata anche la semplice inerzia.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640bis c.p.);

Tal ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente contributi, finanziamenti, mutui agevolati ovvero altre erogazioni, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici, o dall'Unione Europea.

Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640ter c.p.)

Il reato si configura nel caso in cui, alterando, in qualsiasi modo, il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti o ad esso pertinenti si ottenga un ingiusto profitto, in danno dello Stato o di altro Ente Pubblico.

L'alterazione fraudolenta del sistema può essere la conseguenza di un intervento rivolto sia alla componente meccanica dell'elaboratore, sia al software.

Sono considerate pertinenti ad un sistema informatico, e quindi, rilevanti ai sensi della norma in questione, le informazioni contenute su supporti materiali, nonché i dati ed i programmi contenuti su supporti esterni all'elaboratore (come dischi e nastri magnetici o ottici), che siano destinati ad essere utilizzati in un sistema informatico.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si alteri il funzionamento di un sistema informatico o dei dati in esso contenuti al fine di modificare i dati connessi al versamento dei contributi previdenziali.

Concussione (art. 317 c.p.)

Il reato si configura nel momento in cui un PU, ovvero un IPS, abusando della relativa posizione, costringano o inducano taluno a dare o promettere indebitamente, anche in favore di un terzo, denaro o altre utilità non dovute.

Corruzione per un atto d'ufficio (art. 318 c.p.)

Il reato si configura allorquando un Pubblico Ufficiale o un Incaricato di Pubblico Servizio (si veda per quest'ultimo l'articolo 320 c.p.) ricevano per sé o per altri, in denaro o altra utilità, ovvero ne accettino la promessa, una retribuzione non dovuta per compiere, o per aver compiuto, un atto del proprio ufficio.

Il delitto di corruzione si differenzia da quello di concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il reato si configura allorquando un PU o un IPS (si veda per quest'ultimo l'articolo 320 c.p.) ricevano per sé o per altri, in denaro o altra utilità, ovvero ne accettino la promessa, una retribuzione non dovuta per compiere, o per aver compiuto, un atto contrario ai doveri d'ufficio, ovvero per omettere o ritardare (o per avere omesso o ritardato) un atto del proprio ufficio.

Corruzione in atti giudiziari (art. 319ter c.p.)

Il reato si configura nel caso in cui i fatti di corruzione di cui alle fattispecie che precedono siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

E' opportuno evidenziare che nella nozione di PU sono sussumibili, oltre al magistrato, anche altri soggetti quali il cancelliere, i testi e qualsiasi altro funzionario pubblico operante nell'ambito di un contenzioso.

FOCUS SUI DELITTI DI CORRUZIONE

Deve ricordarsi che, essendo i delitti di corruzione fattispecie a c.d. concorso necessario, ai sensi dell'art. 321 c.p., le pene stabilite agli artt. 318, 319, 319 ter si applicano anche al corruttore e non solo al corrotto.

a) Istigazione alla corruzione (art. 322 c.p.)

Il reato si configura nel caso in cui, nei confronti di un PU o di un IPS, sia formulata la promessa o l'offerta di una somma di denaro o di un'altra utilità, qualora la promessa o l'offerta non siano accettate e riguardino, in via alternativa:

- il compimento di un atto d'ufficio;
- l'omissione o il ritardo di un atto d'ufficio;
- il compimento di un atto contrario ai doveri d'ufficio.

È, inoltre, penalmente sanzionata anche la condotta del PU (o IPS) che sollecita una promessa o dazione di denaro o altra utilità da parte di un privato per le medesime finalità.

Induzione indebita a dare o promettere utilità (art. 319^{quater} c.p.)

Il delitto si configura allorquando un pubblico ufficiale oppure un incaricato di pubblico servizio induca taluno a dare o promettere denaro o altra utilità a lui o ad una terza persona, abusando della sua qualità o dei suoi poteri.

Per induzione deve intendersi l'attività di persuasione, convinzione o suggestione, attuata in qualsiasi forma, anche in maniera velata e indiretta, laddove sufficiente ad influire sulla volontà del soggetto passivo

La punibilità è estesa anche a colui che dà o promettere il denaro o altra utilità.

Peculato, concussione, corruzione ed istigazione alla corruzione di membri degli Organi delle Comunità Europee o di Stati esteri (art. 322^{bis} c.p.)

Il reato si configura allorquando la medesima condotta prevista per alcuno dei reati indicati in rubrica venga compiuta da, o nei confronti di, membri degli organi delle Comunità europee o di Stati esteri.

Tali soggetti sono assimilati ai Pubblici Ufficiali qualora esercitino funzioni corrispondenti, e agli Incaricati di Pubblico Servizio negli altri casi.

Quanto alle possibili modalità di commissione del reato, si rinvia alle ipotesi previste, a titolo esemplificativo, per i reati di corruzione e concussione, fermo restando che, ai fini della configurabilità della fattispecie di istigazione, è necessario che l'offerta o la promessa non siano accettate.

Traffico di influenze illecite (art. 346bis c.p.)

La fattispecie incriminatrice in oggetto, rivisitata ed inserita nel Decreto, quale reato presupposto, dalla Legge 3/2019, c.d. Spazzacorrotti, punisce, fuori dei casi di concorso nei reati di corruzione, la condotta di chi, sfruttando o vantando relazioni esistenti o asserite con un p.u./i.p.s. o con uno dei soggetti indicati all'articolo 322 bis c.p., indebitamente si faccia dare o promettere, per sé o per terzi, denaro o altra utilità come prezzo della propria illecita mediazione verso i soggetti pubblici, ovvero per remunerarli.

È punito anche il soggetto che dà o promette.

Ovviamente, non dovrà essere stata esercitata una reale influenza sul soggetto pubblico, altrimenti si verterà, come già si è descritto, nelle ipotesi di corruzione.

4. REATI DI CUI ALLA L. 190/2012

Al fine di ottenere un Modello Organizzativo specificamente improntato alla prevenzione della corruzione è opportuno dedicare attenzione anche a quei reati richiamati dalla L. 190/2012 anche se non normativamente ricompresi tra quelli presupposto per la responsabilità amministrativa degli enti ex D.Lgs. 231/2001.

Si riporta di seguito una sintetica descrizione dei suddetti reati, nonché una breve esposizione delle possibili modalità di attuazione dei reati.

- Peculato (art. 314 c.p.)

Il delitto previsto dal primo comma dell'articolo de quo si configura allorché il pubblico ufficiale o l'incaricato di pubblico servizio, avendo per ragioni d'ufficio o di servizio *“il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria”*. Il delitto di peculato può integrarsi anche nei casi di assenza di danni patrimoniali concretamente apprezzabili, trattandosi infatti di un reato che offende beni giuridici ulteriori quali l'interesse alla legalità, all'imparzialità ed al corretto agire della P.A.

Il secondo comma dell'articolo punisce, per converso, il c.d. “peculato d'uso”, delitto che si verifica nell'ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio si appropri, nelle circostanze succitate, di una *“cosa”* (res specifica; il peculato d'uso non può quindi aversi in presenza di condotta appropriativa di denaro inteso quale bene fungibile o di altri beni fungibili) *“al solo scopo di far[ne] uso momentaneo”*, restituendola immediatamente alla sua funzione originaria.

- **Peculato mediante profitto dell'errore altrui (art. 316 c.p.)**

Il reato punisce il pubblico ufficiale o l'incarico di pubblico servizio che, *“nell'esercizio delle sue funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente per sé o per un terzo denaro o altra utilità”*.

Il delitto de quo si differenzia da quello di cui all'art. 314 c.p. in quanto nel caso qui esaminato la “ricezione” o la “ritenzione” da parte del pubblico ufficiale o dell'incaricato di pubblico servizio avviene durante l'esercizio delle sue funzioni, mediante giovamento dell'errore altrui. L'errore, sull'*an* o sul *quantum debeatur* deve essere spontaneo, preesistente ed indipendente dall'azione del soggetto agente che, consapevole dell'errore, indebitamente (ovverosia in assenza di alcun titolo legittimante) riceve o ritiene la *res*.

- **Abuso d'ufficio (art. 323 c.p.)**

La disposizione in oggetto punisce (fuori dell'ipotesi in cui il fatto costituisca un più grave reato) la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, *“nello svolgimento delle sue funzioni o del servizio, in violazione di norme di legge o regolamento, ovvero omettendo di astenersi”* dinanzi ad un interesse proprio o di un prossimo congiunto o *“negli altri casi prescritti, intenzionalmente procura a sé o altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto”*.

I beni giuridici oggetto di tutela sono costituiti dal buon andamento, dall'imparzialità e dalla trasparenza dell'agire amministrativo, lesi da condotte illegittime non ispirate ad interessi pubblici (tutela della *par condicio civium*).

Il vantaggio ingiusto per come richiamato dalla norma deve essere di natura patrimoniale. Per converso, il danno deve essere solo ingiusto, potendo comportare la lesione di una qualsiasi situazione giuridica soggettiva. Tra condotta dell'agente e l'evento causato deve ovviamente sussistere uno stretto nesso causale (si guardi attentamente all'avverbio *“intenzionalmente”*).

- **Utilizzazione di invenzioni e scoperte conosciute per ragioni d'ufficio (art. 325 c.p.)**

Il delitto in esame è integrato dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che utilizza, a profitto proprio o altrui, invenzioni, scoperte scientifiche o nuove applicazioni industriali destinate a rimanere segrete e delle quali sia venuto a conoscenza per ragione dell'ufficio o del servizio.

- **Rivelazione ed utilizzazione di segreti d'ufficio (art. 326 c.p.)**

Il reato, che può essere commesso anche nella forma dell'agevolazione colposa, è integrato dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che rivela notizie di ufficio, le quali debbono rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, commettendo il fatto in violazione dei doveri inerenti alle funzioni o al servizio esercitato, o comunque abusando della qualità rivestita, ovvero è integrato dalla condotta del pubblico ufficiale o incaricato di un pubblico servizio che si avvale illegittimamente di notizie di ufficio, le quali debbono rimanere segrete, al fine di procurare a sé o ad altri un indebito profitto patrimoniale o al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto.

- **Rifiuto d'atti d'ufficio. Omissione (art. 328 c.p.)**

Il reato in esame comprende due distinte e autonome fattispecie incriminatrici che disciplinano, la prima, l'indebito rifiuto di un'attività "qualificata", per ragioni di giustizia o di sicurezza pubblica, o di ordine pubblico o di igiene e sanità, "indifferibile" e "doverosa" e, la seconda, l'omissione di un atto della pubblica amministrazione espressamente richiesto, con "messa in mora" del funzionario competente alla sua adozione, da parte di chi abbia interesse al suo compimento e la mancata risposta sulle ragioni del ritardo.

- **Interruzione di un servizio pubblico o di pubblica necessità (art. 331 c.p.)**

Il reato in esame è integrato dalle condotte dirette a turbare la regolarità d'un servizio pubblico o di pubblica necessità mediante l'interruzione di esso ovvero mediante la sospensione del lavoro negli

stabilimenti, uffici o aziende ovvero del servizio da parte di coloro che esercitano imprese di servizi pubblici o di pubblica necessità.

- **Turbata libertà degli incanti (art. 353 c.p.)**

La norma è posta a tutela della regolarità delle gare della Pubblica Amministrazione, perciò incrimina l'impedimento o il turbamento di una gara o l'allontanamento dalla stessa di concorrenti che siano realizzati attraverso l'uso di mezzi intimidatori (violenza o minaccia) o fraudolenti (doni, promesse, collusioni e mezzi fraudolenti in genere).

L'ambito di applicazione della norma riguarda solo le ipotesi in cui, in qualsiasi forma, si proceda in forma di gara o licitazione privata, il reato presuppone che vi sia stato inizio della procedura di gara, quindi che almeno sia stato pubblicato il bando, e si realizza quando la gara venga impedita, non potendo essere effettuata a causa di uno dei mezzi suddetti ovvero la gara venga turbata, nel senso che ne venga alterato il regolare svolgimento per influenzarne il risultato rispetto a quello cui si giungerebbe senza l'intervento perturbatore.

5. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITÀ SENSIBILI

In occasione dell'attività di *risk assessment*, sono state individuate, nell'ambito della struttura organizzativa aziendale di SOGERT S.p.A., delle aree considerate “a rischio reato” rispetto alle quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati contro la Pubblica Amministrazione.

Nell'ambito delle aree a rischio reato sono state individuate le attività maggiormente “sensibili”, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in considerazione della sussistenza di rapporti diretti con gli organismi pubblici e/o i soggetti sopra individuati.

Nella tabella seguente è riepilogato il quadro in precedenza esposto.

AREA	MACRO AREA SENSIBILE
Alta direzione	Gestione rapporti con gli enti Pubblici
Alta direzione / Amministrazione / Ufficio legale / Sedi periferiche / Personale	Rapporti con Organi Ispettivi
Alta direzione	Assegnazione e gestione incarichi di consulenza
Alta direzione / Uff. Personale	Ricerca, selezione e assunzione personale
Alta direzione / Uff. Personale	Incentivi al personale
Alta direzione / Amministrazione	Registrazione e pagamento fatture passive
Alta direzione / Amministrazione	Gestione rimborsi spese

6. PRINCIPI COMPORTAMENTALI DA ADOTTARE

I responsabili delle direzioni e delle funzioni coinvolte nelle macro attività “a rischio reato” sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità. Le suddette attività di controllo devono essere adeguatamente formalizzate mediante le apposite schede di evidenza come di seguito specificato.

AREA	MAC RO AREA SENSIBILE	CRITICITA' DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO	PRINCIPI COMPORTAMENTALI	Scheda di evidenza
Alta direzione	Gestione rapporti con gli enti Pubblici	Carenza di una procedura formalizzata che identifichi chiaramente i soggetti che entrano in contatto con i vari Enti pubblici/C omuni ecc. e ne definisca compiti e responsabilità	I rapporti con la P.A./Enti devono essere intrattenuti e gestiti esclusivamente dai responsabili a ciò preposti o da persone incaricate; l'incarico deve altresì contenere indicazioni precise in merito all'oggetto, al settore di competenza della P.A., ecc.	SE-01
Alta direzione / Amministrazione / Ufficio legale / Sedi periferiche / Personale	Rapporti con Organi Ispettivi	Sussiste il rischio di commissione dei reati di corruzione e concussione in quanto la Società o soggetti ad essa appartenenti, al fine di ottenere un trattamento preferenziale in sede di ispezione, potrebbero intrattenere rapporti confidenziali con pubblici dipendenti erogando loro denaro o altre utilità. Il rischio può concretizzarsi, ad esempio, in relazione a verifiche in ambito fiscale, previdenziale, della sicurezza sul lavoro, sanitario, ecc.	Nel caso di ispezioni giudiziarie, tributarie e amministrative i rapporti con gli organi ispettivi devono essere tenuti dai soggetti espressamente delegati per iscritto (di norma il Direttore Generale o il responsabile della funzione interessata). Il delegato deve verificare che gli organi ispettivi redigano verbale delle operazioni compiute e richiederne una copia, in tutti i casi in cui ve ne sia il diritto; la copia dovrà essere adeguatamente conservata. Laddove non sia stato possibile ottenere il rilascio di copia del verbale ispettivo, il soggetto delegato a partecipare all'ispezione provvederà a redigere un verbale ad uso interno. Il personale della società, nell'ambito delle proprie competenze, deve prestare piena collaborazione, nel rispetto della legge, allo svolgimento delle attività ispettive.	SE-01
Alta direzione	Assegnazione e gestione incarichi di consulenza	Sussiste il rischio di commissione di condotte corruttive nel processo di assegnazione di incarichi o consulenze al fine di veicolare denaro o altre utilità verso soggetti pubblici o soggetti in grado di influenzare le scelte di soggetti pubblici, con il fine unico o prevalente di apportare vantaggi alla Società.	I consulenti e i collaboratori devono essere individuati sulla base di precisi requisiti di onorabilità, professionalità e competenza ed in relazione alla loro reputazione e affidabilità. I contratti devono essere definiti per iscritto in tutte le condizioni e termini. I compensi dei consulenti e collaboratori devono trovare adeguata giustificazione nell'incarico conferito e devono essere congrui in considerazione dei prezzi di mercato e delle tariffe vigenti. I contratti conclusi devono contenere: a) curriculum della persona selezionata e eventuali ulteriori curriculum dei vari candidati; b) una apposita dichiarazione con la quale consulenti e collaboratori affermino di essere a conoscenza delle norme di cui al Decreto e si impegnino a rispettarle; c) dichiarazione con la quale si impegnino a rispettare i principi contenuti nel Codice Etico della Società o i valori comuni cui il presente Codice si ispira; d) una apposita clausola risolutiva espressa che regoli le conseguenze della violazione da parte di consulenti e collaboratori degli obblighi di cui ai punti precedenti; e) dichiarazione del Direttore Generale con la quale si segnala l'esigenza aziendale di conferire incarico, che il costo pattuito è in linea con il mercato e che verificherà l'output dell'attività conferita.	SE-02
Alta direzione / Uff. Personale	Ricerca, selezione e assunzione personale	Sussiste il rischio di commissione di condotte corruttive mediante l'assunzione di personale avente rapporti diretti o indiretti con soggetti appartenenti alla P.A. ovvero con ex esponenti della PA	Nei processi di assunzione del personale deve essere garantita l'applicazione di criteri di valutazione dei candidati che risponda alle esigenze di obiettività e trasparenza. In particolare il processo di ricerca assunzione e selezione deve avvenire nel rigoroso rispetto delle procedure standard definite dall'azienda per la selezione del personale; l'esito del processo valutativo dei candidati deve essere formalizzato in apposita documentazione, archiviata a cura del Responsabile competente secondo le procedure interne.	SE-03
Alta direzione / Uff. Personale	Incentivi al personale	Sussiste il rischio di commissione di condotte corruttive mediante la promozione e l'incentivazione di personale avente rapporti diretti o indiretti con soggetti appartenenti alla P.A. ovvero con ex esponenti della PA	Nei processi di promozione e incentivazione del personale deve essere garantita l'applicazione di criteri oggettivi di valutazione del personale attraverso: a) la definizione degli incentivi in fase contrattuale; b) definizione dell'ammontare oggetto di incentivazione e degli obiettivi da raggiungere; c) il monitoraggio e la predisposizione di valutazioni da parte dei responsabili di area; d) l'esito del processo valutativo del personale deve essere formalizzato in apposita documentazione e archiviata a cura del Responsabile competente.	SE-04
Alta direzione / Amministrazione	Registrazione e pagamento fatture passive	Sussiste il rischio di commissione di reati societari connessi a false scritture contabili e di creazione di fondi di denaro occulti mediante operazioni di fatturazione/pagamento per forniture inesistenti; ovvero, mediante l'acquisto di beni o servizi presso fornitori che abbiano rapporti preferenziali con soggetti appartenenti alla P.A. è possibile ottenere, indirettamente, vantaggi per la società.	Le operazioni di rilevazione e registrazione delle attività di impresa devono essere effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza. I Pagamenti delle fatture devono essere autorizzati a valle della verifica della consegna della merce o della prestazione del servizio	SE-05
Alta direzione / Amministrazione	Gestione rimborsi spese	Sussiste il rischio di creazione di fondi neri per fini corruttivi attraverso registrazioni di rimborsi spese relativi a missioni e trasferite per importi superiori a quello reale o a fronte di missioni inesistenti	E' necessario che siano preventivamente stabiliti, in funzione della natura della prestazione svolta, limiti quantitativi al rimborso di spese sostenute da parte del personale della società. Il rimborso delle spese sostenute deve essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute.	SE-06

I responsabili delle direzioni e delle funzioni coinvolte nelle macro attività “a rischio reato” sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate e conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico di SOGERT S.p.A., nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità, al rispetto delle norme di comportamento di seguito indicate.

E’ fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dagli artt. 24 e 25 del Decreto;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di porre in essere o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con il Consorzio, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse del Consorzio e nel pieno rispetto delle norme del Codice Etico;
- di elargire, offrire o promettere denaro a pubblici ufficiali o incaricati di pubblico servizio;
- di distribuire, offrire o promettere omaggi e regali che non siano di modico valore, in violazione di quanto previsto dal Codice Etico e dalla prassi aziendale. Oltre che di modico valore, atti di cortesia commerciale, quali omaggi o forme di ospitalità, o qualsiasi altra forma di beneficio (anche sotto forma di liberalità) in favore dei Pubblici Ufficiali sono consentiti soltanto se non compromettano l’integrità e la reputazione delle parti e da non poter essere interpretati da un osservatore terzo ed imparziale, come atti destinati a garantire vantaggi e favori in modo improprio. Qualsiasi destinatario che riceva direttamente o indirettamente richieste di benefici da Pubblici Ufficiali deve immediatamente segnalare la circostanza all’Organismo di Controllo.
- di accordare, offrire o promettere altri vantaggi, di qualsiasi natura essi siano, in favore di pubblici ufficiali o incaricati di pubblico servizio è fatto divieto ai destinatari di distogliere il Pubblico Ufficiale dallo svolgimento delle proprie incombenze, promettendo o coinvolgendolo in attività di svago, viaggi e/o sollevandolo dai propri compiti eseguendone le attività;
- di effettuare prestazioni in favore dei Partner e/o dei consulenti e/o dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto lavorativo con essi costituito;
- di riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- di presentare dichiarazioni e/o attestazioni non veritiere a organismi pubblici, nazionali o comunitari, al fine di conseguire e/o usufruire di erogazioni pubbliche, contributi, finanziamenti agevolati od altre provvidenze, ovvero per l’ottenimento di licenze, autorizzazioni, concessioni, etc. per le quali

non ricorrano in capo al Consorzio o al proprio Personale i requisiti soggettivi e/o oggettivi all'uopo richiesti da norme di legge o regolamentari come condizione per la loro concessione;

- destinare le somme ricevute da enti pubblici, nazionali o comunitari, a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli cui erano destinati, o non darne fedele e veritiera rendicontazione.

Tutta la documentazione relativa alle trattative e ai contatti con la Pubblica Amministrazione deve essere conservata per permettere verifiche da parte dell'Organismo di Controllo.

E' vietato a tutti i Destinatari promettere o dare direttamente o per interposta persona incarichi di collaborazione a Pubblici Ufficiali che abbiano, o abbiano avuto nel biennio precedente, un ruolo decisionale in situazioni in cui il Consorzio abbia o abbia avuto un interesse o un vantaggio. Eventuali richieste in tal senso da parte del Pubblico Ufficiale devono essere segnalate all'Organismo di Controllo.

E' inoltre vietato qualsiasi comportamento, anche attraverso interposta persona, finalizzato a influenzare l'indipendenza di giudizio del Pubblico Ufficiale, finalizzato a distoglierlo dal servizio esclusivo alla Pubblica Amministrazione, a violare le regole di disciplina ed onore della stessa o i principi di buon andamento e imparzialità della Pubblica Amministrazione.

E' altresì vietato qualsiasi comportamento finalizzato ad assicurare un qualsiasi illecito vantaggio al Consorzio o al Destinatario.

I soggetti deputati alle funzioni di controllo e supervisione devono porre particolare attenzione all'attuazione degli adempimenti connessi all'espletamento di tali operazioni e riferire immediatamente all'OdV, eventuali situazioni di irregolarità rilevate o ad essi segnalate;

E' necessario effettuare verifiche informatiche periodiche, allo scopo di evidenziare i soggetti che hanno la libera disponibilità di mezzi informatici aventi contatti con l'esterno (trasmissione telematica dei dati, in modo particolare se corredata di autenticazione o firma digitale, invio di file prodotti da elaborazioni *on line*, *etc*); Laddove un Pubblico Ufficiale sfrutti la posizione che ricopre per ottenere da parte dei Destinatari o del Consorzio utilità che non gli spettino, deve essere data immediata informazione all'Organismo di Controllo a mezzo segnalazione.

7. RESPONSABILITÀ E REPORTISTICA ALL'ORGANISMO DI VIGILANZA

Ogni scostamento, anche lieve, dalle procedure operative rilevato dai destinatari del presente Modello dovrà essere immediatamente riferito per iscritto all'OdV tramite la apposita casella di posta elettronica o, in subordine, a mezzo di raccomandata interna con sottoscrizione di chi riceve.

Devono essere previsti controlli a campione sui processi a rischio, sulla base di un piano annuale di controlli approvato dall'OdV.

A tal fine, in relazione alle macro attività sensibili “a rischio reato”, sono individuati e nominati da parte dell’OdV uno o più Responsabili Interni per ciascuna area, cui sarà richiesto di gestire il flusso informativo verso l’OdV in merito allo svolgimento delle attività aziendali (Schede di Evidenza).

Le Schede di Evidenza sono costituite dai rapporti in formato elettronico (foglio elettronico) deputati a supportare le diverse funzioni nella formalizzazione delle attività aziendali.

Tali rapporti, direttamente accessibili da parte dell’OdV consentono a quest’ultimo il miglioramento della propria attività di monitoraggio del Modello.

L’OdV cura l’emanazione e l’aggiornamento delle Schede di Evidenza in funzione delle sue specifiche esigenze di vigilanza. In particolare l’OdV, nell’ambito della propria attività, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all’esigenza di prevenire la commissione dei reati contro la Pubblica Amministrazione, previsti dal D.lgs. n. 231/2001;
- vigilare sull’effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi sub responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l’adeguatezza e/o l’effettività.

L’OdV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati contro la Pubblica Amministrazione, al Consiglio Direttivo ed al Collegio Sindacale, secondo i termini indicati nel Regolamento dell’Organismo di Vigilanza.

	Protocollo Etico – Organizzativo	PRO.2
	Gestione della sicurezza sul luogo di lavoro	

INDICE

1. SCOPO	2
2. AMBITO DI APPLICAZIONE	2
3. REATI DI CUI ALL'ART. 25 SEPTIES DEL D.LGS. N. 231/2001	2
4. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITA' SENSIBILI	4
5. PRINCIPI COMPORTAMENTALI DA ADOTTARE	5
6. RESPONSABILITÀ E REPORTISTICA ALL'ORGANISMO DI VIGILANZA	7

INDICE DELLE REVISIONI				
REV	DATA	OGGETTO	REDATTO *** da ...	APPROVATO da ...

1. SCOPO

La presente norma comportamentale ha lo scopo di illustrare i principi che devono essere seguiti nella gestione della sicurezza sul lavoro e nella predisposizione della relativa documentazione.

2. AMBITO DI APPLICAZIONE

La norma si applica a tutte le Funzioni aziendali che, nell'espletamento delle attività di propria competenza, si trovino a dover intervenire, a qualunque titolo, sulla tutela dell'igiene e della salute sul lavoro; in particolare:

- sicurezza all'interno della società SOGERT S.p.A.;
- sicurezza e igiene sui luoghi di lavoro in genere;

3. REATI DI CUI ALL'ART. 25 SEPTIES DEL D.LGS. N. 231/2001

Si riporta di seguito una sintetica descrizione dei reati richiamati nell'art. 25^{septies} del Decreto, fermo restando che, ai sensi dell'art. 26 del Decreto, la Società potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

In via preliminare, si riporta il testo dell'art. 25^{septies}, così che possa apparire più agevole il rinvio alla norma di diritto penale:

1. In relazione al delitto di cui all'**articolo 589 del codice penale**, commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

2. Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

3. In relazione al delitto di cui all'**articolo 590, terzo comma**, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non

superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi.

Art. 589 c.p. - Omicidio colposo.

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Se il fatto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.

Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

Art. 590 c.p. - Lesioni personali colpose

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni.

Se i fatti di cui al secondo comma sono commessi nell'esercizio abusivo di una professione per la quale è richiesta una speciale abilitazione dello Stato o di un'arte sanitaria, la pena per lesioni gravi è della reclusione da sei mesi a due anni e la pena per lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

4. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITA' SENSIBILI

In occasione dell'attività di *risk assessment*, sono state individuate, nell'ambito della struttura organizzativa aziendale di SOGERT, delle aree considerate "a rischio reato" rispetto alle quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati di cui sopra (omicidio colposo e lesioni colpose gravi o gravissime, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro).

Nell'ambito dell' unica area a rischio reato è stata individuata una macro-attività maggiormente "sensibile", ovvero un'attività al cui espletamento è connesso il rischio di commissione dei reati anche in considerazione delle disposizioni contenute nel nuovo T.U. 81/2008.

Nella tabella seguente è riepilogato il quadro in precedenza esposto.

AREA	MACRO AREA SENSIBILE
Alta Direzione	Gestione salute e sicurezza sui luoghi di lavoro

5. PRINCIPI COMPORTAMENTALI DA ADOTTARE

I responsabili delle direzioni e delle funzioni coinvolte nella macro attività "a rischio reato" sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità, con il fine ultimo di una valutazione globale e documentata di tutti i rischi per la salute e sicurezza dei lavoratori presenti nell'ambito dell'organizzazione, finalizzata ad individuare le adeguate misure di prevenzione e/o protezione nonché ad elaborare il programma delle misure atte a garantire il miglioramento nel tempo dei livelli di salute e sicurezza.

Le suddette attività di controllo devono essere adeguatamente formalizzate mediante le apposite schede di evidenza come di seguito specificato.

AREA	MACRO AREA SENSIBILE	CRITICITA' DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO	PRINCIPI COMPORTAMENTALI	Scheda di evidenza
Alta Direzione	Gestione salute e sicurezza sui luoghi di lavoro	Corretta attuazione delle misure di prevenzione in base alla normativa vigente	a) sono correttamente nominati i soggetti previsti dalla normativa in materia di igiene e sicurezza dei luoghi di lavoro e sono loro conferiti correttamente i poteri necessari allo svolgimento del ruolo agli stessi assegnato; b) ove previsto, sono effettuate le necessarie comunicazioni alle autorità competenti; c) la scelta di eventuali consulenti esterni e dei soggetti previsti in materia di igiene e sicurezza dei luoghi di lavoro (tra cui, il responsabile del Servizio di prevenzione e protezione, il medico competente, eventuale personale tecnico, etc.) avviene sulla base di requisiti di professionalità e competenza, anche in riferimento a quanto previsto dalla legge (in particolare dal D.Lgs. 81/2008 e relative norme collegate e di attuazione) e, in riferimento a essi, la scelta è motivata per iscritto; d) la valutazione dei rischi deve essere costante e periodicamente revisionata ed aggiornata; le verifiche ai fini di eventuali revisioni devono avvenire almeno annualmente e, in ogni caso, ogni qualvolta si verificano dei mutamenti significativi nell'organizzazione del lavoro e/o dei luoghi di lavoro; e) in linea con le previsioni dettate dalla normativa vigente, la valutazione dei rischi viene svolta dal datore di lavoro, il quale si avvale del supporto di altri soggetti quali il Responsabile del Servizio di Prevenzione e Protezione e del Medico Competente, previa consultazione del Rappresentante dei Lavoratori per la Sicurezza; f) le misure di prevenzione e protezione dai rischi devono essere adeguate, aggiornate ed effettivamente attuate; g) le procedure e i manuali di gestione delle emergenze, così come richiesti dalla normativa vigente, devono essere adeguati ed effettivamente attuati; h) gli infortuni sul lavoro e le relative cause devono essere registrati, monitorati ed analizzati al fine di ridurre l'incidenza; i) è previsto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.	SE-07

Si precisa che l'art. 26 T.U. 81/2008:

Il datore di lavoro, in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a lavoratori autonomi all'interno della propria azienda, o di una singola unità produttiva della stessa, nonché nell'ambito dell'intero ciclo produttivo dell'azienda medesima, sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo:

a) verifica, con le modalità previste dal decreto di cui all'art. 6, comma 8, lettera g), l'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione. Fino alla data di entrata in vigore del decreto di cui al periodo che precede, la verifica è eseguita attraverso le seguenti modalità:

- 1) acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato;*
- 2) acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico-professionale, ai sensi dell'articolo 47 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445;*

b) fornisce agli stessi soggetti dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività.

I responsabili delle direzioni e delle funzioni coinvolte nelle macro attività “a rischio reato” sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate e conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico di SOGERT, nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità, al rispetto delle norme di comportamento di seguito indicate.

E' fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dall’art. 25septies del Decreto;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di porre in essere o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con la società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della società e nel pieno rispetto delle norme del Codice Etico;

- tutta la documentazione relativa alla sicurezza sul luogo di lavoro anche in virtù di novità legislative) deve essere conservata per permettere verifiche da parte dell'Organismo di Controllo;

I soggetti deputati alle funzioni di controllo e supervisione devono porre particolare attenzione all'attuazione degli adempimenti connessi all'espletamento di tali operazioni e riferire immediatamente all'OdV, eventuali situazioni di irregolarità rilevate o ad essi segnalate.

6. RESPONSABILITA' E REPORTISTICA ALL'ORGANISMO DI VIGILANZA

Ogni scostamento, anche lieve, dalle procedure operative rilevato dai destinatari del presente Modello dovrà essere immediatamente riferito per iscritto all'OdV tramite la apposita casella di posta elettronica o, in subordine, a mezzo di raccomandata interna con sottoscrizione di chi riceve.

Devono essere previsti controlli a campione sui processi a rischio, sulla base di un piano annuale di controlli approvato dall'OdV.

A tal fine, in relazione alle macro attività sensibili "a rischio reato", sono individuati e nominati da parte dell'OdV uno o più Responsabili Interni per ciascuna area, cui sarà richiesto di gestire il flusso informativo verso l'OdV in merito allo svolgimento delle attività aziendali (Schede di Evidenza).

Le Schede di Evidenza sono costituite dai rapporti in formato elettronico (foglio elettronico) deputati a supportare le diverse funzioni nella formalizzazione delle attività aziendali.

Tali rapporti, direttamente accessibili da parte dell'OdV consentono a quest'ultimo il miglioramento della propria attività di monitoraggio del Modello.

L'OdV cura l'emanazione e l'aggiornamento delle Schede di Evidenza in funzione delle sue specifiche esigenze di vigilanza. In particolare l'OdV, nell'ambito della propria attività, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati previsti dall'art. 25^{septies} del D.lgs. n. 231/2001 e, comunque, il non rispetto di quanto previsto dal T.U. 81/2008;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi sub responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;

- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati per la sicurezza ed igiene sul luogo di lavoro al Comitato Direttivo ed al Collegio Sindacale, secondo i termini indicati nel Regolamento dell'Organismo di Vigilanza.

	Protocollo Etico – Organizzativo	PRO.3
	Prevenzione Reati Informatici	

INDICE

1. SCOPO	2
2. AMBITO DI APPLICAZIONE	3
3. REATI DI CUI AGLI ARTT 24 BIS D.LGS. N. 231/2001	3
4. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITA' SENSIBILI	4
5. PRINCIPI COMPORTAMENTALI DA ADOTTARE	5
6. RESPONSABILITÀ E REPORTISTICA ALL'ORGANISMO DI VIGILANZA	6

INDICE DELLE REVISIONI				
REV	DATA	OGGETTO	REDATTO da ...	APPROVATO da ...

1. SCOPO

La presente norma comportamentale ha lo scopo di illustrare i principi che devono essere seguiti nella gestione dei sistemi informatici e nel trattamento dei dati sensibili.

2. AMBITO DI APPLICAZIONE

La norma si applica a tutte le Funzioni aziendali che, nell'espletamento delle attività di propria competenza, si trovino ad avere accesso a sistemi informatici e alla rete internet, nonché a gestire dati sensibili dei contribuenti, in merito, in via esemplificativa, a:

- gestione dei contratti;
- gestione dei dati sensibili.

3. REATI DI CUI AGLI ARTT. 24 BIS E 25 NOVIES DEL D.LGS. N. 231/2001

Si riporta di seguito una sintetica descrizione di alcuni dei reati richiamati dagli articoli 24 bis e 25 novies del Decreto, fermo restando che, ai sensi dell'art. 26 del Decreto, la Società potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

Accesso abusivo ad un sistema informatico o telematico (art. 615 ter cod. pen.)

Il reato si configura qualora un soggetto si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantenga contro la volontà espressa di chi ha diritto di escluderlo.

La condotta è aggravata se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o violazione dei doveri.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater cod. pen.)

Il reato si configura quando un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies cod. pen.)

Il reato si configura quando un soggetto, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegna o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater cod. pen.)

Il reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa.

Il reato si configura anche qualora un soggetto riveli al pubblico, mediante qualsiasi mezzo di informazione, il contenuto delle comunicazioni suddette.

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies cod. pen.)

Il reato si configura qualora un soggetto installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis cod. pen.)

Il reato si configura qualora un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

Danneggiamento di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter cod. pen.)

Il reato si configura qualora un soggetto commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Danneggiamento di sistemi informatici o telematici (art. 635 quater cod. pen.)

Il reato si configura qualora un soggetto distruggendo, deteriorando, cancellando, alterando o sopprimendo informazioni, dati o programmi informatici, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies cod. pen.)

Il reato si configura qualora un soggetto distruggendo, deteriorando, cancellando, alterando o sopprimendo informazioni, dati o programmi informatici, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità.

Documenti informatici (art. 491 bis cod. pen.)

Il reato si configura qualora venga commessa una delle falsità previste dal capo III titolo IV del libro III del codice penale e riguardi un documento informatico pubblico o privato avente efficacia probatoria.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies cod. pen.)

Il reato si configura qualora un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Violazione delle norme in materia di Perimetro di Sicurezza Nazionale Cibernetica (Art. 11 D.L. 105/2019, così come convertito dalla L. 133/2019)

Nel corso del 2020 dovrebbe trovare definizione la disciplina in materia di Sicurezza Nazionale Cibernetica. In particolare, essa si applicherà alle amministrazioni pubbliche, agli enti ovvero operatori nazionali da cui dipende l'esercizio di una funzione essenziale dello Stato nonché la prestazione di un servizio preminente per il mantenimento di attività civili, sociali o economiche fondamentali per lo Stato e dal cui malfunzionamento, interruzione ovvero utilizzo improprio possa discendere un pericolo per la sicurezza nazionale.

La puntuale individuazione dei soggetti tenuti al rispetto delle norme, nonché dell'elenco delle procedure vincolanti, è stata rimessa a decreti non ancora emanati.

I destinatari saranno altresì sottoposti all'attività di ispezione e vigilanza della Presidenza del Consiglio dei Ministri, in caso di enti pubblici e pubblici economici, ovvero del Ministero dello Sviluppo Economico, laddove si tratti di soggetti di natura privatistica.

Gli stessi dovranno poi rispettare obblighi informativi e procedurali: 1) predisporre e aggiornare, con cadenza almeno annuale, un elenco delle reti, dei sistemi informativi e dei servizi informatici di propria pertinenza, dal cui malfunzionamento o interruzione ovvero utilizzo improprio possa derivare un pregiudizio per gli interessi dello Stato; 2) nel caso in cui intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi, nonché per

l'espletamento di servizi informatici di interesse collettivo, dovranno comunicarlo al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello Sviluppo Economico.

A tal proposito, occorre precisare come il Decreto 231 preveda quale reato presupposto, se commesso nell'interesse o vantaggio dell'ente, la condotta di chiunque fornisca informazioni, dati o elementi di fatto non rispondenti al vero, ovvero ometta di comunicarli, in violazione degli obblighi summenzionati, al fine di ostacolare o condizionare le attività di controllo e vigilanza poc'anzi enucleate.

Art. 171 L. 633/1941, 1° comma, lettera a) bis e terzo comma

La norma tutela il diritto di sfruttamento di un'opera in capo al titolare, vietando, quindi, la messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa.

Art. 171 bis L. 633/1941

La norma punisce l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore (il c.d. software), nonché l'importazione, la distribuzione, la vendita o la detenzione, a scopo commerciale o imprenditoriale, o la concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE, ivi inclusa la predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori. Analogo discorso vale per l'abusiva riproduzione, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o dimostrazione in pubblico del contenuto di una banca dati, l'estrazione od il reimpiego della banca dati, nonché la distribuzione, la vendita o la concessione in locazione di banche di dati.

Art. 171 ter L. 633/1941

La norma tutela i "format" televisivi, la musica, la letteratura, le opere cinematografiche etc., vietando, in particolare, l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o di ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; la riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Art. 171 septies L. 633/1941

La norma sanziona la mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o la falsa dichiarazione, ovvero di quei supporti contenenti programmi per elaboratore disciplinati dal decreto legislativo 29 dicembre 1992, n. 518, utilizzati esclusivamente mediante elaboratore elettronico, sempre che tali programmi non contengano suoni, voci o sequenze di immagini in movimento tali da costituire opere fonografiche, cinematografiche o audiovisive intere, non realizzate espressamente per il programma per elaboratore, ovvero loro brani o parti eccedenti il cinquanta per cento dell'opera intera da cui sono tratti, che diano luogo a concorrenza all'utilizzazione economica delle opere medesime.

Art. 171 octies L. 633/1941

La norma sanziona, infine, la fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

4. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITA' SENSIBILI

In occasione dell'attività di risk assesment, sono state individuate, nell'ambito della struttura organizzativa aziendale di SOGERT S.p.A., delle aree considerate "a rischio reato" rispetto alle quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati di cui sopra (danneggiamento di informazioni, dati e programmi informatici, danneggiamento di informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità, danneggiamento di sistemi informatici o telematici, danneggiamento di sistemi informatici o telematici di pubblica utilità, frode informatica con sostituzione di identità digitale, indebito utilizzo di strumenti di prelievo o di pagamento altrui, falsificazione di carte di credito o altri strumenti di prelievo o di pagamento, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante, omissione nell'adozione delle misure di sicurezza, inosservanza di provvedimenti del Garante).

Nell'ambito delle aree a rischio reato sono state individuate le attività maggiormente "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in considerazione della sussistenza di operazioni potenzialmente a rischio.

Nella tabella seguente è riepilogato il quadro in precedenza esposto.

Area	Macroarea sensibile
Alta direzione / Amministrazione / Ufficio legale / Sedi periferiche / Personale	Utilizzo rete
	Inserimento dati

5. PRINCIPI COMPORTAMENTALI DA ADOTTARE

I responsabili delle direzioni e delle funzioni coinvolte nelle macro attività “a rischio reato” sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità. Le suddette attività di controllo devono essere adeguatamente formalizzate mediante le apposite schede di evidenza come di seguito specificato.

Macroarea sensibile	Criticità del sistema organizzativo e di controllo	Principi comportamentali	Scheda di Evidenza
Utilizzo rete	Rigide restrizioni di accesso alla rete ed ai software aziendali	Il responsabile informatico deve prevedere un elenco di azioni non effettuabili in rete, nonché un elenco di siti inaccessibili e il blocco a determinati software che possano utilizzare la rete in modo inappropriato. Il detto responsabile, individuato con apposita procedura nel rispetto della normativa vigente (anche di natura regolamentare), dovrà essere fornito di apposita delega e vigilare sull’eventuale elusione delle predette restrizioni.	SE - 08
Inserimento dati	Assegnazione ad ogni singolo dipendente di un account personale per accedere alle postazioni	Ad ogni singolo dipendente deve essere assegnato un account con password personale per poter accedere alla propria postazione, con generazione di password mensile, per consentire la tracciabilità degli accessi.	SE - 09
	Cronologia delle operazioni effettuate dai singoli account per poter risalire al dipendente che ha effettuato operazioni sospette	Il responsabile informatico deve poter risalire all’account del dipendente che ha inserito, modificato, alterato, scaricato i dati contenuti nel gestionale di riferimento.	

I responsabili delle direzioni e delle funzioni coinvolte nelle macro attività “a rischio reato” sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate e conformi ai principi indicati dal Modello e, in particolare, dal Codice Etico di SOGERT S.p.A., nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità.

E’ fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dall’art. 24 bis del Decreto;

- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di porre in essere o agevolare operazioni in conflitto di interesse – effettivo o potenziale – con la Società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della Società e nel pieno rispetto del Codice Etico.

Tutta la documentazione relativa alla gestione delle procedure informatiche e del trattamento dei dati sensibili (anche in virtù di novità legislative) deve essere conservata per permettere verifiche da parte dell'Organismo di Vigilanza.

I soggetti deputati alle funzioni di controllo e supervisione devono porre particolare attenzione all'attuazione degli adempimenti connessi all'espletamento di tali operazioni e riferire immediatamente all'OdV eventuali situazioni di irregolarità rilevate o ad essi segnalate.

E' necessario effettuare verifiche informatiche periodiche, allo scopo di evidenziare i soggetti che hanno la libera disponibilità di mezzi informatici aventi contatti con l'esterno (trasmissione telematica dei dati, in modo particolare se corredata di autenticazione o firma digitale, invio di file prodotti da elaborazioni on line, etc.).

E' inoltre necessario prevedere l'attuazione di una corretta politica delle password, degli accessi e degli altri strumenti informatici.

6. RESPONSABILITA' E REPORTISTICA ALL'ORGANISMO DI VIGILANZA

Ogni scostamento, anche lieve, dalle procedure operative rilevato dai destinatari del presente Modello dovrà essere immediatamente riferito per iscritto all'OdV tramite la apposita casella di posta elettronica o, in subordine, a mezzo di raccomandata interna con sottoscrizione di chi riceve.

Devono essere previsti controlli a campione sui processi a rischio, sulla base di un piano annuale di controlli approvato dall'OdV.

A tal fine, in relazione alle macro attività sensibili "a rischio reato", sono individuati e nominati da parte dell'OdV uno o più Responsabili Interni per ciascuna area, cui sarà richiesto di gestire il flusso informativo verso l'OdV in merito allo svolgimento delle attività aziendali (Schede di Evidenza).

Le Schede di Evidenza sono costituite dai rapporti in formato elettronico (foglio elettronico) deputati a supportare le diverse funzioni nella formalizzazione delle attività aziendali.

Tali rapporti, direttamente accessibili da parte dell'OdV consentono a quest'ultimo il miglioramento della propria attività di monitoraggio del Modello.

L'OdV cura l'emanazione e l'aggiornamento delle Schede di Evidenza in funzione delle sue specifiche esigenze di vigilanza. In particolare l'OdV, nell'ambito della propria attività, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati contro la Pubblica Amministrazione, previsti dal D.lgs. n. 231/2001;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi sub responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati informatici, al Consiglio Direttivo ed al Collegio Sindacale, secondo i termini indicati nel Regolamento dell'Organismo di Vigilanza.

	Protocollo Etico – Organizzativo	PRO.4
	Prevenzione Reati Tributari	

INDICE

1. SCOPO	2
2. AMBITO DI APPLICAZIONE	3
3. REATI DI CUI ALL'ART. 25 QUINQUIESDECIES D.LGS. N. 231/2001	3
4. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITÀ SENSIBILI	5
5. PRINCIPI COMPORTAMENTALI DA ADOTTARE	7
6. RESPONSABILITÀ E REPORTISTICA ALL'ORGANISMO DI VIGILANZA	8

INDICE DELLE REVISIONI				
REV	DATA	OGGETTO	REDATTO da ...	APPROVATO da ...

1. SCOPO

La presente norma comportamentale ha lo scopo di illustrare i principi che devono essere seguiti nella prevenzione dei reati tributari e nella predisposizione della relativa documentazione.

Preliminarmente, è opportuno esporre le ragioni sottese alla introduzione, tra i reati presupposto della responsabilità amministrativa da reato degli enti, di alcune tra le fattispecie incriminatrici previste dal Decreto Legislativo n. 74/2000, rubricato “*Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205*”.

A tal proposito, è d'uopo evidenziare che l'innovazione legislativa è stata attuata su sollecitazione eurounitaria, per il tramite del D.L. n.124/2019, successivamente convertito con modificazioni dalla Legge n. 157/2019. Infatti, il nostro legislatore si è adeguato agli obblighi derivanti dalla Direttiva n. 2017/1371 (c.d. Direttiva PIF) approvata dal Parlamento Europeo in data 5 luglio 2017, con cui è stato richiesto agli Stati membri di predisporre minime misure necessarie al fine di prevenire e reprimere i reati lesivi degli interessi finanziari dell'Unione, commessi nell'interesse o a vantaggio delle persone giuridiche.

Il Parlamento Italiano, cogliendo l'occasione, ha esteso la portata dell'intervento necessitato (che a ben vedere avrebbe dovuto attingere più propriamente le frodi in materia di IVA), allargando il novero dei reati presupposto, risolvendo una serie di criticità, come si vedrà di qui ad un attimo.

Sicché, il nuovo art. 25 quinquiesdecies del Decreto ha previsto, quali reati presupposto: a) il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, ex articolo 2, commi 1 e 2 bis D.Lgs. n. 74/2000; b) il delitto di dichiarazione fraudolenta mediante altri artifici, ex art. 3 D.Lgs. n. 74/2000; c) il delitto di emissione di fatture o altri documenti per operazioni inesistenti, ex art. 8, commi 1 e 2 bis D. Lgs. n. 74/2000; d) il delitto di occultamento o distruzione di documenti contabili, ex art. 10 D.Lgs. n. 74/2000; e) il delitto di sottrazione fraudolenta al pagamento di imposte, ex art. 11 D.Lgs. n. 74/2000.

Come è stato preannunciato, con il predetto intervento, il legislatore interno ha scelto di porre fine ad una serie di problematiche; in particolare, hanno trovato soluzione i problemi interpretativi sintetizzati dalla nota sentenza c.d. Gubert (Cass. Pen. SS.UU. n. 10561 del 30 gennaio 2014) in materia di confisca e sequestro preventivo del profitto derivante da reato tributario, commesso nell'interesse o a vantaggio di un ente.

Si ricorderà che il Supremo Consesso aveva ritenuto come, a seguito della commissione di reati tributari a vantaggio o nell'interesse di una persona giuridica, potesse unicamente procedersi alla confisca diretta (e, prima, al sequestro preventivo) del profitto, ove nella disponibilità della società. Per converso, sulla base del tenore letterale dell'articolo 322 ter c.p., non poteva procedersi alla confisca per equivalente (e, prima, al sequestro preventivo), in quanto misura non prevista dalla legge, salvo i casi in cui l'ente fosse mero schermo della persona fisica.

Con la riforma del 2019, il legislatore ha eliminato ogni dubbio, rendendo obbligatoria la misura ablativa avente ad oggetto il profitto del reato, anche per equivalente.

2. AMBITO DI APPLICAZIONE

La norma si applica a tutte le Funzioni aziendali che, nell'espletamento delle attività di propria competenza, si trovino a dover gestire, in via esemplificativa, i seguenti processi:

- rapporti contrattuali con controparti;
- processo di approvvigionamento di beni e/o servizi;
- pagamenti (focus in particolare su retribuzioni, compensi, rimborsi spese);
- contabilità;
- fatture e altri documenti contabili;
- presentazione delle dichiarazioni;
- rapporto con eventuali consulenti esterni in materia fiscale;
- operazioni straordinarie;
- emissione di assegni;
- formazione ed informazione del personale.

3. REATI DI CUI ALL'ART. 25 QUINQUESDECIES DEL D.LGS. N. 231/2001

Si riporta di seguito una sintetica descrizione di alcuni dei reati richiamati dall'art. 25 quinquiesdecies del Decreto, fermo restando che, ai sensi dell'art. 26 del Decreto, SO.GE. R.T S.p.A. potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, commi 1 e 2bis D.Lgs. n. 74/2000)

L'articolo 2 del D.Lgs. n. 74/2000 punisce la condotta di chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, utilizzando fatture o altri documenti (con analogo rilievo probatorio) per operazioni inesistenti, indichi elementi passivi fittizi in una delle qualsiasi dichiarazioni relative alle menzionate imposte.

Occorre evidenziare che, con l'espressione "*fatture o altri documenti per operazioni inesistenti*", si fa riferimento tanto ai casi di emissione a fronte di operazioni mai effettuate in tutto o in parte, quanto a quelli in cui siano indicati quali partecipanti dell'operazione soggetti diversi da quelli effettivi, nonché a quelli in cui siano riportati corrispettivi o importi iva in misura differente rispetto a quelli reali.

Il comma 2 bis dell'art. 2 prevede, invece, limiti edittali inferiori ove l'ammontare degli elementi passivi fittizi sia inferiore ad euro cento mila.

Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)

La fattispecie incriminatrice punisce la condotta di chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, per il tramite di operazioni simulate oggettivamente o soggettivamente ovvero utilizzando documenti falsi o altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indichi in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, realizzando congiuntamente le seguenti condizioni: a) imposta evasa superiore, con riferimento a taluna delle singole imposte, a euro trentamila; b) ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, sia superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2 bis D. Lgs. n. 74/2000)

L'articolo 8 del D.Lgs. n. 74/2000 punisce la condotta di chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emetta o rilasci fatture o altri documenti per operazioni inesistenti. Con la locuzione "*altri documenti*" ci si riferisce a quelli aventi natura probatoria sotto il profilo fiscale. Il reato punisce ogni tipo di divergenza sussistente tra la realtà commerciale e la relativa documentazione, non già l'esclusiva inesistenza totale dell'operazione. Il comma 2 bis prevede, invece, limiti edittali inferiori ove l'importo non rispondente al vero indicato sia, per periodo d'imposta, inferiore ad euro cento mila.

Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)

La fattispecie incriminatrice, d'applicazione residuale, giusta la clausola di sussidiarietà espressa ("*salvo che il fatto costituisca più grave reato*") prevede la punizione di chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulti o distrugga, in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari (quest'ultima è una condizione obiettiva di punibilità). La norma tutela il corretto esercizio della funzione di accertamento fiscale, sicché il delitto si consuma allorquando si determini l'impossibilità di ricostruire il volume d'affari o i redditi.

Secondo la giurisprudenza, peraltro, il delitto si configura altresì qualora la verifica tributaria sia resa anche solo più difficoltosa in virtù delle condotte citate.

Inoltre, occorre precisare che l'”impossibilità di ricostruire” può essere tanto assoluta quanto relativa.

La fattispecie incriminatrice, cioè, trova applicazione anche nelle ipotesi in cui possa comunque ricostruirsi il volume d'affari o dei redditi, purché ciò avvenga aliunde, fuori del perimetro della documentazione da conservare da parte del reo.

Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)

L'articolo 11 punisce la condotta di chi, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte, per un ammontare complessivo superiore ad euro cinquantamila, alieni simulatamente o compia altri atti fraudolenti sui propri o altrui beni, in maniera idonea a rendere inefficace, anche in parte, la procedura di riscossione coattiva.

È prevista altresì, al comma 2, la punizione di chi, al fine di ottenere per se' o per altri un pagamento parziale dei tributi e relativi accessori, indichi nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo nonché elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

La fattispecie incriminatrice tutela l'Erario, essendo volta a salvaguardare la garanzia patrimoniale sui beni del debitore.

Per la consumazione del delitto di cui al comma 1, non è necessaria la preesistenza di un debito tributario.

Si tratta infatti di un reato di pericolo, che si configura allorquando siano posti in essere atti fraudolenti idonei a vanificare una probabile futura procedura di riscossione.

Tuttavia, al fine di evitare la sindacabilità di ogni atto dispositivo, per la consumazione del reato deve ritenersi che il contribuente debba avere quanto meno la conoscenza di un'attività di accertamento in atto da parte dell'Amministrazione.

4. AREE POTENZIALMENTE A "RISCHIO REATO" E MACRO ATTIVITA' SENSIBILI

In occasione dell'attività di risk assessment, nell'ambito della struttura organizzativa aziendale di SO.GE.R.T. S.p.A., sono state individuate delle aree considerate “a rischio reato” rispetto alle quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati tributari.

Nell'ambito delle aree a rischio reato sono state individuate le attività maggiormente “sensibili”, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in questione.

Nella tabella seguente è riepilogato il quadro in precedenza esposto.

Area	Macroarea sensibile
Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità	- Rapporti con controparti; - Approvvigionamento di beni e servizi; - Pagamenti.
	- Contabilità; - Fatture e altri documenti contabili; - Presentazione delle dichiarazioni; - Rapporti con eventuali consulenti esterni in materia fiscale.
	- Operazioni straordinarie; - Emissione di assegni.
	- Formazione ed informazione del personale

5. PRINCIPI COMPORTAMENTALI DA ADOTTARE

I responsabili delle aree nelle macro attività “a rischio reato” sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità.

Le suddette attività di controllo devono essere adeguatamente formalizzate mediante le apposite schede di evidenza come di seguito specificato.

Area	Macroarea sensibile	Criticità del sistema organizzativo e di controllo	Principi comportamentali	Scheda di Evidenza
Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità	- Rapporti con controparti; - Approvvigionamento di beni e servizi; - Pagamenti.	Sussiste il rischio di commissione dei reati tributari, ad esempio mediante fatturazioni oggettivamente ovvero soggettivamente inesistenti o recanti corrispettivi o importi iva differenti rispetto a quelli reali. Inoltre, può accadere che i pagamenti effettuati siano di importo inferiore rispetto a quanto dichiarato o certificato, come nel caso della corresponsione degli stipendi.	- In primo luogo occorre rispettare i principi comportamentali indicati nei precedenti protocolli. - In particolare, occorre che le controparti siano scelte a seguito di verifiche sulla loro affidabilità, operatività e sui prezzi. - Quando si ricevono prestazioni di beni o servizi, è necessario registrare tutto quanto possa consentire il riscontro della loro effettività. Inoltre, al momento dell'effettuazione dei pagamenti occorre riscontrare la coincidenza tra chi ha effettuato la prestazione e il destinatario della corresponsione, nonché la congruità delle fatture ricevute rispetto al versamento. - Quando si effettuano prestazioni di beni e servizi occorre conservare tutto quanto provi la loro effettività (es. comunicazioni, mail, contratti, etc). E' inoltre importante dare evidenza delle procedure di pricing, nonché chiedere alla controparte una dichiarazione che attesti di aver ricevuto i beni o i servizi oggetto di affidamento. - Infine, è indispensabile verificare il corretto importo delle fatture, nonché la loro legittima provenienza. - Con riferimento ai pagamenti verso i dipendenti, è opportuno che ognuno di essi dichiari, all'atto della ricezione della busta paga, quanto effettivamente percepito. Le spese sostenute per finalità societarie, come è noto, saranno rimborsate previa esibizione di documentazione idonea. - In generale, dunque, si impone di controllare la regolarità delle procedure di approvvigionamento, prestando particolare riferimento alle necessità societarie, all'effettività degli scambi beni - servizi contro prezzo, nonché alla corrispondenza tra pattuizioni e risorse economiche, al controllo della correttezza degli adempimenti fiscali e contabili. - È indispensabile, infine, garantire la segregazione delle funzioni, con formalizzazione di incarichi e poteri, nonché la tracciabilità dell'intero iter.	SE - 10
	- Contabilità; - Fatture e altri documenti contabili; - P - Presentazione delle dichiarazioni; - Rapporti con eventuali consulenti esterni in materia fiscale.	Sussiste il rischio di commissione dei reati tributari, ad esempio per il mezzo dell'utilizzo di fatture o altri documenti per operazioni inesistenti, ovvero per l'occultamento o la distruzione della documentazione contabile.	- Occorre innanzitutto il rispetto dei principi stabiliti nei protocolli già menzionati. - È necessario che siano indicati i luoghi di tenuta di tutta la documentazione contabile obbligatoria, nonché i soggetti formalmente incaricati della loro predisposizione, tenuta e conservazione. - È necessario delegare formalmente i soggetti preposti a dialogare con l'A.F., anche nei casi di controlli ed ispezioni, nel rispetto del principio della segregazione delle funzioni. Analogamente per i casi di trasmissione di dichiarazioni e comunicazioni. - Ove ci si avvalga della consulenza di esperti in materia fiscale, è necessario che la loro scelta avvenga nel rispetto dei comuni principi, con evidenza degli incarichi e delle deleghe loro attribuite e premurandosi di documentare ogni passaggio.	SE - 11
	- Operazioni straordinarie; - Emissione di assegni.	Sussiste il rischio di commissione dei reati tributari, ad esempio mediante atti fraudolenti su beni aziendali, al fine di sottrarli ad una probabile procedura esecutiva.	- È necessario che prima di ogni operazione straordinaria vi sia un dialogo preliminare tra CdA, Collegio Sindacale, ed Odv, al fine di riscontrarne l'opportunità, gli identificativi dei soggetti coinvolti, la documentazione a supporto delle operazioni. E' opportuno ascoltare i preposti ai rapporti con le Autorità nei casi di ispezioni e controlli di natura fiscale. - Infine, ogni emissione di assegni dovrà trovare giustificazione.	SE - 12
	- Formazione ed informazione del personale	La commissione dei reati tributari potrebbe essere agevolata dalla mancata conoscenza del personale.	- È necessario che periodicamente il personale sia adeguatamente formato ed informato.	SE - 14

È fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dall' art. 25 quinquiesdecies del Decreto;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di porre in essere o agevolare operazioni in conflitto di interesse – effettivo o potenziale – con la Società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della Società e nel pieno rispetto del Codice Etico.

Tutta la documentazione relativa a quanto suesposto deve essere conservata per permettere verifiche da parte

dell'Organismo di Vigilanza.

I soggetti deputati alle funzioni di controllo e supervisione devono porre particolare attenzione all'attuazione degli adempimenti connessi all'espletamento di tali operazioni e riferire immediatamente all'OdV eventuali situazioni di irregolarità rilevate o ad essi segnalate.

6. RESPONSABILITÀ E REPORTISTICA ALL'ORGANISMO DI VIGILANZA

Ogni scostamento, anche lieve, dalle procedure operative rilevato dai destinatari del presente Modello dovrà essere immediatamente riferito per iscritto all'OdV tramite la apposita casella di posta elettronica o, in subordine, a mezzo di raccomandata interna con sottoscrizione di chi riceve.

Devono essere previsti controlli a campione sui processi a rischio, sulla base di un piano annuale di controlli approvato dall'OdV.

A tal fine, in relazione alle macro attività sensibili "a rischio reato", sono individuati e nominati da parte dell'OdV uno o più Responsabili Interni per ciascuna area, cui sarà richiesto di gestire il flusso informativo verso l'OdV in merito allo svolgimento delle attività aziendali (Schede di Evidenza).

Le Schede di Evidenza sono costituite dai rapporti in formato elettronico (foglio elettronico) deputati a supportare le diverse funzioni nella formalizzazione delle attività aziendali.

Tali rapporti, direttamente accessibili da parte dell'OdV consentono a quest'ultimo il miglioramento della propria attività di monitoraggio del Modello.

L'OdV cura l'emanazione e l'aggiornamento delle Schede di Evidenza in funzione delle sue specifiche esigenze di vigilanza. In particolare, l'OdV, nell'ambito della propria attività, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati tributari previsti dal D.Lgs. n. 231/2001;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
 - verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi sub responsabili, nonché le procedure aziendali vigenti;
 - comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
 - curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'OdV deve comunicare i risultati della propria attività di vigilanza e controllo al Consiglio di Amministrazione, secondo i termini indicati nel Regolamento dell'Organismo di Vigilanza.

**SCHEDA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE E DEI REATI
CONTRO LA PUBBLICA AMMINISTRAZIONE
(ART.25 D.LGS. 231/2001)
*(Ref. Protocollo 1; Paragrafo 5)***

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Direttore Generale o responsabile di Area

D) Processo sensibile: Gestione dei rapporti con gli Enti Pubblici - Gestione delle visite ispettive da parte di pubblici ufficiali o incaricati del servizio pubblico

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

I rapporti con la P.A./Enti devono essere intrattenuti e gestiti esclusivamente dai responsabili a ciò preposti o da persone incaricate; l'incarico deve altresì contenere indicazioni precise in merito all'oggetto, al settore di competenza della P.A., ecc.

Nel caso di ispezioni giudiziarie, tributarie e amministrative i rapporti con gli organi ispettivi devono essere tenuti dai soggetti espressamente delegati per iscritto (di norma il Direttore Generale o il responsabile della funzione interessata). Il delegato deve verificare che gli organi ispettivi redigano verbale delle operazioni compiute e richiederne una copia, in tutti i casi in cui ve ne sia il diritto; la copia dovrà essere adeguatamente conservata. Laddove non sia stato possibile ottenere il rilascio di copia del verbale ispettivo, il soggetto delegato a partecipare all'ispezione provvederà a redigere un verbale ad uso interno. Il personale della società, nell'ambito delle proprie

	SOGERT S.p.A.	SE – 01
	Scheda Evidenza	

competenze, deve prestare piena collaborazione, nel rispetto della legge, allo svolgimento delle attività ispettive.

1) Indicazione della P.A. o ente con cui si intrattengono rapporti.

2) Indicazione dei funzionari della P.A. o dell'ente pubblico con cui s'intrattiene il rapporto.

3) Descrizione della finalità aziendale del rapporto con la P.A. o l'ente pubblico.

4) Cronologia delle attività poste in essere ai fini della realizzazione dell'Operazione Sensibile.

5) Preposti alla specifica attività con la P.A.

6) Richieste avanzate ed esito del rapporto intrattenuto con l'amministrazione.

	SOGERT S.p.A.	SE – 01
	Scheda Evidenza	

- 7) Allagare copia del verbale delle operazioni compiute dall'organo ispettivo e/o verbale predisposto ad uso interno. Fornire indicazioni relative alla conservazione.

- 8) Fornire informazioni sullo svolgimento dell'ispezione in corso e dei rapporti intrattenuti a qualsiasi titolo con i funzionari pubblici fino alla chiusura dell'attività ispettiva (ad es. incontri, comunicazioni, richieste ecc.)

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla Sogert S.p.A.”.

F.TO IL RESPONSABILE DELL'OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 1
	Scheda Evidenza	

SCHEMA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI REATI CONTRO
LA PUBBLICA AMMINISTRAZIONE
(ART.25 D.LGS. 231/2001)
(Ref. Protocollo 1; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Alta Direzione

D) Processo sensibile: **Assegnazione e gestione incarichi di consulenza**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

I consulenti e i collaboratori devono essere individuati sulla base di precisi requisiti di onorabilità, professionalità e competenza ed in relazione alla loro reputazione e affidabilità. I contratti devono essere definiti per iscritto in tutte le condizioni e termini. I compensi dei consulenti e collaboratori devono trovare adeguata giustificazione nell'incarico conferito e devono essere congrui in considerazione dei prezzi di mercato e delle tariffe vigenti.

- 1) Motivazione dell'assegnazione dell'incarico al consulente esterno, indicazione dell'oggetto del contratto e verifica della congruità dello compenso pattuito:

--

	SOGERT S.p.A.	SE – 1
	Scheda Evidenza	

2) curriculum del consulente selezionato e motivazioni della scelta;

3) Dichiarazione di conoscenza delle norme di cui al Decreto 231/2001 e di impegno al rispetto delle stesse da parte del consulente; Dichiarazione del rispetto dei principi contenuti nel Codice Etico della Società; Specifica informativa circa la clausola risolutiva espressa in caso di violazione degli obblighi di cui ai punti precedenti;

4) Verifica da parte del Responsabile dell'Operazione Sensibile dell'output generato (per le attività continuative la verifica dovrà avvenire annualmente).

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla società Sogert S.p.A.”.

F.TO IL RESPONSABILE DELL'OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 03
	Scheda Evidenza	

SCHEDA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI REATI CONTRO
LA PUBBLICA AMMINISTRAZIONE
(ART.25 D.LGS. 231/2001)
(Ref. Protocollo 1; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Alta direzione / Uff. Personale

D) Processo sensibile: **Ricerca, selezione e assunzione personale**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Nei processi di assunzione del personale deve essere garantita l'applicazione di criteri di valutazione dei candidati che risponda alle esigenze di obiettività e trasparenza. In particolare il processo di ricerca assunzione e selezione deve avvenire nel rigoroso rispetto delle procedure standard definite dall'azienda per la selezione del personale; l'esito del processo valutativo dei candidati deve essere formalizzato in apposita documentazione, archiviata a cura del Responsabile competente secondo le procedure interne.

1) Motivazione dell'esigenza della nuova assunzione e del profilo professionale ricercato:

	SOGERT S.p.A.	SE – 03
	Scheda Evidenza	

- 2) curriculum del candidato scelto e motivazioni della scelta con particolare riferimento agli altri candidati selezionati;

- 3) Dichiarazione di avvenuto ricevimento del REGOLAMENTO INTERNO AZIENDALE e di essere a conoscenza delle norme di cui al Decreto 231/2001 e dei principi contenuti nel Codice Etico della società;

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla società Sogert S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 04
	Scheda Evidenza	

SCHEDA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI REATI CONTRO
LA PUBBLICA AMMINISTRAZIONE
(ART.25 D.LGS. 231/2001)
(Ref. Protocollo 1; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. “Sub Responsabile”), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Alta direzione / Uff. Personale

D) Processo sensibile: **Incentivi al personale**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Il responsabile della gestione del personale nella macro attività “a rischio reato” è tenuto, nei processi di promozione e incentivazione del personale a garantire l'applicazione di criteri oggettivi di valutazione del personale. la formalizzazione e l'archiviazione, a cura del Responsabile competente, dell'esito del processo valutativo del personale.

1) Indicazione degli incentivi definiti in fase contrattuale e eventuali incentivi definiti successivamente:

--

- 2) Definizione dell'ammontare oggetto di incentivazione e degli obiettivi da raggiungere (*integrare eventuali allegati*):

- 3) Predisposizione della valutazione da parte della Direzione aziendale:

- 4) Formalizzazione e archiviazione, a cura del Responsabile competente, dell'esito del processo valutativo del personale:

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla società Sogert S.p.A.”.

F.TO IL RESPONSABILE DELL'OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 05
	Scheda Evidenza	

SCHEMA DI EVIDENZA ATTIVITÀ A RISCHIO
E DEI REATI CONTRO LA PUBBLICA AMMINISTRAZIONE
(ART.25 D.LGS. 231/2001)
(Ref. Protocollo 1; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Alta direzione / Amministrazione

D) Processo sensibile: **Tenuta della contabilità – ciclo passivo**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Il responsabile dell'area Amministrativa è tenuto ad effettuare le operazioni di rilevazione e registrazione delle attività di impresa secondo correttezza e nel rispetto del principio di veridicità, completezza e accuratezza.

- 1) I pagamenti sono stati effettuati previa autorizzazione e dopo la verifica della corrispondenza dell'avvenuta prestazione di servizio o consegna della merce con l'ordine/contratto (evidenziare eventuali difformità su base mensile/trimestrale allegando documentazione di supporto)

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla società Sogert S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 06
	Scheda Evidenza	

SCHEMA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI
CONTRO LA PUBBLICA AMMINISTRAZIONE
(ART.25 D.LGS. 231/2001)
(Ref. Protocollo 1; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Alta direzione / Amministrazione

D) Processo sensibile: **Gestione rimborsi spese**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Il responsabile dell'Area Amministrativa nello svolgimento delle operazioni relative alla gestione rimborsi spese dovrà assicurarsi che gli stessi siano dimostrabili e conformi ai limiti quantitativi previsti dal regolamento interno del personale.

- 1) I rimborsi spese sono stati liquidati previa produzione di documentazione giustificativa e utilizzando specifica modulistica. Inoltre, sono stati verificati, per natura di spesa, i limiti quantitativi approvati dall'organo Amministrativo della Società (evidenziare eventuali difformità su base mensile/trimestrale allegando documentazione di supporto).

	SOGERT S.p.A.	SE – 06
	Scheda Evidenza	

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla società Sogert S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE-07
	Scheda Evidenza	

SCHEDA DI EVIDENZA ATTIVITÀ A RISCHIO

PROTOCOLLO DI PREVENZIONE DEL REATO DI OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(ART.25^{septies} D.LGS. 231/2001)

(Ref. Protocollo 4; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: Alta Direzione

D) Processo sensibile: **Gestione salute e sicurezza sui luoghi di lavoro**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

I responsabili della direzione e delle aree coinvolte nella macro attività "a rischio reato" sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, nonché al controllo che i suddetti principi siano rispettati da tutti i dipendenti che operano sotto la loro responsabilità, con il fine ultimo di una valutazione globale e documentata di tutti i rischi per la salute e sicurezza dei lavoratori presenti nell'ambito dell'organizzazione, finalizzata ad individuare le adeguate misure di prevenzione e/o protezione nonché ad elaborare il programma delle misure atte a garantire il miglioramento nel tempo dei livelli di salute e sicurezza.

La scelta di eventuali consulenti esterni e dei soggetti previsti in materia di igiene e sicurezza dei luoghi di lavoro (tra cui, il responsabile del Servizio di prevenzione e protezione, il medico competente, eventuale personale tecnico, etc.) deve avvenire sulla base di requisiti di professionalità e competenza, anche in riferimento a quanto previsto dalla legge (in particolare dal D.lgs. 81/2008 e relative norme collegate e di attuazione) e, in riferimento a essi, la scelta deve essere motivata per iscritto.

- 1) curriculum del candidato individuato ad assumere il ruolo di responsabile della sicurezza e motivazioni della scelta;

- 2) Indicazioni delle comunicazioni periodiche alle Autorità competenti ove previsto dalla legge;

- 3) Revisione ed aggiornamento periodico della valutazione dei rischi; (le verifiche devono avvenire almeno annualmente e, in ogni caso, ogni qualvolta si verificano mutamenti significativi nell'organizzazione del lavoro e/o dei luoghi di lavoro)

- 4) Conferma dell'adeguatezza delle misure di prevenzione e protezione dai rischi e della loro effettiva attuazione nonché dell'adeguatezza delle procedure e dei manuali di gestione delle emergenze;

- 5) Indicazione degli infortuni sul lavoro intervenuti nel periodo (annuale) e delle relative cause;

- 6) Rendiconto sulla riunione periodica di cui all'art. 35 del D.lgs. 81/2008, ove applicabile (indicazioni riportate anche nel verbale di riunione periodica che deve essere stilato nell'occasione);

--

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla SOGERT S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT	SE – 08
	Scheda Evidenza	

SCHEDA DI EVIDENZA DI ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI REATI INFORMATICI
(ART. 24 BIS D.LGS. 231/01)
(Ref. protocollo 3, Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile ("Responsabile Interno"):

Il Responsabile è munito di delega ? SI NO

B) Indicazione di eventuali soggetti nominati dal Responsabile Interno (c.d. "Sub Responsabili Interni"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE, DURATA E OGGETTO DELEGA

C) Macroarea aziendale di riferimento: ALTA DIREZIONE / AMMINISTRAZIONE / UFFICIO LEGALE / SEDI PERIFERICHE / PERSONALE

D) Tipologia/Oggetto dell'Operazione sensibile: UTILIZZO DELLA RETE INTERNET

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Il responsabile informatico deve prevedere un elenco di azioni non effettuabili in rete, nonché un elenco di siti inaccessibili e il blocco a determinati software che possano utilizzare la rete in modo inappropriato. Il detto responsabile, individuato con apposita procedura nel rispetto della normativa vigente (anche di natura regolamentare), dovrà essere fornito di apposita delega e vigilare sull'eventuale elusione delle predette restrizioni.

1) Modalità di scelta del responsabile informatico:

	SOGERT	SE – 08
	Scheda Evidenza	

- 2) Rendiconto annuale dell'avvenuta formazione e informazione dei lavoratori, dei preposti, dei dirigenti, nonché degli altri soggetti eventualmente autorizzati all'utilizzo dei Sistemi Informatici, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio della rete internet:

- 3) Rendiconto annuale delle verifiche effettuate sui Sistemi Informatici in uso ai lavoratori, ai preposti, ai dirigenti, nonché agli altri soggetti eventualmente autorizzati all'utilizzo:

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D. Lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.Lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.Lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato da SOGERT S.p.A.”.

F.TO IL RESPONSABILE DELL'OPERAZIONE

luogo - - - data

	SOGERT	SE – 09
	Scheda Evidenza	

SCHEDA DI EVIDENZA DI ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI REATI INFORMATICI
(ART. 24 BIS D.LGS. 231/2001)
(Ref. protocollo 3; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile ("Responsabile Interno"):

Il Responsabile è munito di delega ? SI NO

B) Indicazione di eventuali soggetti nominati dal Responsabile Interno (c.d. "Sub Responsabili Interni"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE, DURATA E OGGETTO DELEGA

C) Macroarea aziendale di riferimento: ALTA DIREZIONE / AMMINISTRAZIONE / UFFICIO LEGALE / SEDI PERIFERICHE / PERSONALE

D) Tipologia/Oggetto dell'Operazione sensibile: INSERIMENTO DATI

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Ad ogni singolo dipendente deve essere assegnato un account con password personale per poter accedere alla propria postazione, con generazione di password mensile, per consentire la tracciabilità degli accessi, così che il responsabile informatico possa risalire all'account del dipendente che ha inserito, scaricato i dati contenuti ne gestionale di riferimento.

- 1) Verifica della corretta assegnazione delle password di accesso al personale dipendente, nonché del sistema di generazione automatica periodica della stessa. Verifica periodica (trimestrale) degli accessi consentiti ai dipendenti in base alla propria configurazione. Segnalare eventuali anomalie:

--

	SOGERT	SE – 09
	Scheda Evidenza	

- 2) Verifica di eventuali operazioni non autorizzate compiute da dipendenti relativamente all'utilizzo dei Sistemi Informatici (es. inserimento, modifica, alterazione, acquisizione di dati sensibili). Indicare le eventuali anomalie riscontrate:

--

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D. Lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.Lgs. 231/2001 descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.Lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato da SOGERT S.p.A.”.

F.TO IL RESPONSABILE DELL'OPERAZIONE

luogo - - - data

	SOGERT S.p.A.	SE – 10
	Scheda Evidenza	

SCHEMA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI TRIBUTARI
(ART. 25 QUINQUESDECIES D.LGS. 231/2001)
(Ref. Protocollo 4; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: **Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità**

D) Processo sensibile: **Rapporti con controparti; approvvigionamento di beni e servizi; pagamenti.**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

In primo luogo, occorre rispettare i principi comportamentali indicati nei precedenti protocolli.

In particolare, occorre che le controparti siano scelte a seguito di verifiche sulla loro affidabilità, operatività e sui prezzi.

Inoltre, quando si ricevono prestazioni di beni o servizi, è necessario registrare tutto quanto possa consentire il riscontro della loro effettività (es. bando, contratto, comunicazioni etc.).

Al momento dell'effettuazione dei pagamenti occorre riscontrare la coincidenza tra chi ha effettuato la prestazione e il destinatario della corresponsione, nonché la congruità delle fatture ricevute rispetto al versamento.

	SOGERT S.p.A.	SE – 10
	Scheda Evidenza	

Particolare attenzione deve essere prestata per le ipotesi di rifornimento di carburante ai mezzi di trasporto. E' opportuna, a questo fine, la tenuta del registro relativo al parco mezzi.

Quando si effettuano prestazioni di beni e servizi occorre conservare tutto quanto provi la loro effettività (es. comunicazioni, mail, contratti, etc). È inoltre importante dare evidenza delle procedure di pricing, nonché chiedere alla controparte una dichiarazione che attesi di aver ricevuto i beni o i servizi oggetto di affidamento.

Infine, è indispensabile verificare il corretto importo delle fatture, nonché la loro legittima provenienza.

Con riferimento ai pagamenti verso i dipendenti, è opportuno che ognuno di essi dichiari, all'atto della ricezione della busta paga, quanto effettivamente percepito. Le spese sostenute per finalità societarie, come è noto, saranno rimborsate previa esibizione di documentazione idonea.

In generale, dunque, si impone di controllare la regolarità delle procedure di approvvigionamento, prestando particolare riferimento alle necessità societarie, all'effettività degli scambi beni - servizi contro prezzo, nonché alla corrispondenza tra pattuizioni e risorse economiche, al controllo della correttezza degli adempimenti fiscali e contabili.

È indispensabile, infine, garantire la segregazione delle funzioni, con formalizzazione di incarichi e poteri, nonché la tracciabilità dell'intero iter.

- 1) Dare evidenza della formalizzazione degli incarichi attribuiti.

	SOGERT S.p.A.	SE – 10
	Scheda Evidenza	

- 2) Indicare quale documentazione viene conservata in relazione alle singole operazioni con controparti contrattuali, ai pagamenti nei confronti del personale, alla gestione dei rimborsi spese.

- 3) Indicare i controlli espletati prima di procedere a pagamenti e/o fatturazioni.

- 4) Indicare le eventuali criticità riscontrate con relative azioni intraprese.

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001, descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla SO.GE.R.T. S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 11
	Scheda Evidenza	

SCHEMA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI TRIBUTARI
(ART. 25 QUINQUIESDECIES D.LGS. 231/2001)
(Ref. Protocollo 4; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: **Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità**

D) Processo sensibile: **Contabilità; fatture e altri documenti contabili; presentazione delle dichiarazioni; rapporti con eventuali consulenti esterni in materia fiscale.**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

Occorre innanzitutto il rispetto dei principi stabiliti nei protocolli già menzionati.

È necessario che siano indicati i luoghi di tenuta di tutta la documentazione contabile obbligatoria, nonché i soggetti formalmente incaricati della loro predisposizione, tenuta e conservazione.

È necessario delegare formalmente i soggetti preposti a dialogare con l'A.F., anche nei casi di controlli ed ispezioni, nel rispetto del principio della segregazione delle funzioni. Analogamente per i casi di trasmissione di dichiarazioni e comunicazioni.

Infine, ove ci si avvalga della consulenza di esperti in materia fiscale, è necessario che la loro scelta avvenga nel rispetto dei comuni principi, con evidenza degli incarichi e delle deleghe loro attribuite e premurandosi di documentare ogni passaggio.

- 1) Dare evidenza della formalizzazione degli incarichi attribuiti, anche in relazione al rapporto con l'A.F. nei casi di ispezioni e controlli.

- 2) Indicare dove è conservata la documentazione contabile obbligatoria, con indicazione dei soggetti incaricati della loro predisposizione, tenuta, conservazione.

- 3) Indicare i riferimenti di eventuali consulenti esterni in materia fiscale, specificandone ruoli, attribuzioni, competenze.

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001, descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla SO.GE.R.T. S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 12
	Scheda Evidenza	

SCHEDA DI EVIDENZA ATTIVITA' A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI TRIBUTARI
(ART. 25 QUINQUIESDECIES D.LGS. 231/2001)
(Ref. Protocollo 4; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: **Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità**

D) Processo sensibile: **Operazioni straordinarie; emissione di assegni.**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

È necessario che prima di ogni operazione straordinaria vi sia un dialogo preliminare tra CdA, Collegio Sindacale, revisori ed OdV, al fine di riscontrarne l'opportunità, gli identificativi dei soggetti coinvolti, la documentazione a supporto delle operazioni. È opportuno ascoltare i preposti ai rapporti con le Autorità nei casi di ispezioni e controlli di natura fiscale.

Infine, ogni emissione di assegni dovrà trovare giustificazione.

1) Indicare se e quali operazioni straordinarie vi siano state.

--

- 2) Ove vi siano state operazioni straordinarie, evidenziarne l'opportunità, la modalità di espletamento, le identità delle controparti, nonché l'intero iter seguito. Occorre specificare quali Organi societari sono stati coinvolti nelle valutazioni, nonché le risultanze dell'interrogazione del personale preposto ai rapporti con l'A.F.

- 3) Specificare per quali fini sono stati emessi assegni, indicando il soggetto preposto alle operazioni. Fornire evidenza documentale.

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001, descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla SO.GE.R.T. S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data

	SOGERT S.p.A.	SE – 13
	Scheda Evidenza	

SCHEDA DI EVIDENZA ATTIVITÀ A RISCHIO
PROTOCOLLO DI PREVENZIONE DEI TRIBUTARI
(ART. 25 QUINQUIESDECIES D.LGS. 231/2001)
(Ref. Protocollo 4; Paragrafo 5)

A) Nome del responsabile dell'Operazione Sensibile:

B) Indicazione di eventuali soggetti nominati dal Responsabile (c.d. "Sub Responsabile"), cui vengono delegate, con riferimento all'Operazione Sensibile, le funzioni di seguito indicate:

NOMINATIVO SUB-RESPONSABILE	FUNZIONE / OGGETTO DELEGA

C) Macroarea aziendale di riferimento: **Organo amministrativo - Direzione - Responsabili di Area - Ufficio contabilità**

D) Processo sensibile: **Formazione ed informazione del personale.**

E) Principio comportamentale da seguire nell'esecuzione dell'Operazione Sensibile:

È necessario che periodicamente il personale sia adeguatamente formato ed informato.

- 1) Dare evidenza dell'attività formativa ed informativa espletata nei confronti del personale.

	SOGERT S.p.A.	SE – 13
	Scheda Evidenza	

Assunzione di impegno, da parte del Responsabile Interno, al rispetto delle norme del D.lgs. 231/2001:

“Io sottoscritto _____, Responsabile Interno della suddetta operazione sensibile ai fini dell’attuazione del Modello di organizzazione e di gestione ai sensi del D.lgs. 231/2001, descritta nella presente Scheda Evidenza, dichiaro di conoscere e di aver preso atto delle previsioni di cui al D.lgs. 231/2001 e successive integrazioni. Io sottoscritto mi impegno, nell’effettuazione di tutti gli adempimenti connessi all’esecuzione dell’Operazione Sensibile, a tenere un comportamento conforme al principio comportamentale prescritto nel protocollo di comportamento in riferimento all’operazione sensibile nonché dei principi generali di comportamento previsti nel Modello Organizzativo di gestione e controllo adottato dalla SO.GE.R.T. S.p.A.”.

F.TO IL RESPONSABILE DELL’OPERAZIONE

luogo e data



Società di Gestione Riscossione Tributi

Sistema di Gestione Privacy
“Registro delle attività”
ai sensi del Regolamento 679/2016 in materia di privacy

REV	DATA	CAUSALE	APPROVATO	FIRMA
Mod Rev 00 Sistema di gestione privacy	03/01/2019	EMISSIONE DOCUMENTO	Amministratore	

SOMMARIO

00 PREMESSA	4
1.0 FONTI NORMATIVE	5
1.1 GDPR - REGOLAMENTO EU 2016/679	5
1.2 CODICE DELLA PRIVACY 196/2003	6
1.3 TERMINI E DEFINIZIONI	7
2.0 SOGERT SI PRESENTA: ASPETTI GENERALI.....	10
2.1 DATA PROTECTION IN AZIENDA	13
2.2 IL REGISTRO DEI TRATTAMENTI	14
3.0 METODOLOGIA PER L'ANALISI DEI RISCHI.....	15
3.1 PREMESSA	16
3.2 ASSET	16
3.3 PRE-ASSESSMENT E RISK-ASSESSMENT	17
4.0 MODALITA'DI TRATTAMENTO DEI DATI	18
4.1 TIPOLOGIA DI DATI	18
4.2 PRESCRIZIONI	22
5.0 DALL'ANALISI DEI RISCHI ALLE MISURE TECNICHE ED ORGANIZZATIVE AZIENDA	25
5.1 STRUTTURA ORGANIZZATIVA	26
5.2 SOGGETTI DELLA PRIVACY: DETERMINAZIONE DEI COMPITI E RUOLI	27
5.3 ORGANIGRAMMA DELLE RESPONSABILITA'	34
5.4 AREA TECNOLOGICA.....	36
6.0 VERIFICA SULL'ADEGUATEZZA DELLE MISURE	38

7.0 DATI DI CONTATTO.....	41
7.1 ELENCO IINCARICATI	42

ALLEGATI

- 1) Allegato (A) Analisi dei rischi (RISK ASSESSMENT)
- 2) Modulistica da Mod. 2Privacy rev a Mod.26 Pivacy rev. (informative, contratti, procedure) in formato digitale .

PREMESSA

Il diritto alla protezione della sfera privata di un individuo contro le ingerenze altrui, soprattutto da parte dello Stato, è stato sancito per la prima volta da uno strumento giuridico internazionale nell'articolo 12 della Dichiarazione universale dei diritti dell'uomo (UDHR) delle Nazioni Unite (ONU) del 1948 riguardante il rispetto della vita privata e familiare. Una dichiarazione che ha prodotto un eco di riforme legislative che si sono succedute e che hanno tenuto conto del progresso sociale, economico e soprattutto tecnologico. Il concetto di diritto alla privacy cambia nel tempo, cambia perchè l'uomo è cambiato, interagisce con il mondo, utilizza gli strumenti che offre la tecnologia.

Sono trascorsi due secoli da quando i giuristi Warren e Brandeis si batterono per il riconoscimento giuridico di una privacy che toccava la sfera privata, il diritto di essere lasciato da solo, (Right to be let alone); oggi l'uomo utilizza Internet, e-mail, cellulari e, inevitabilmente, lascia tracce durante l'utilizzo, pertanto le esigenze cambiano, e nuovi diritti si affermano. Il diritto alla privacy, come il diritto alla tutela dei dati, si incontrano inevitabilmente con altri diritti che riguardano i rapporti di lavoro, con tutte le problematiche che ne derivano, quando ci sono ad es. trattamenti dei dati con strumenti di videosorveglianza. I soggetti sottoposti a tali trattamenti esigono particolare protezione che il Legislatore, specie in questi ultimi anni, ha cercato di assicurare; allo stesso tempo, non sono mancati gli interventi del Garante della Privacy, che più volte ha richiamato l'attenzione alla tutela della sfera dei diritti personali.

*In Italia le esigenze di garanzia, di trasparenza e di tutela hanno trovato una adeguata normativa con il Codice della Privacy 196/2003. Il mercato sempre più globale e le esigenze di tutela transnazionale hanno portato il legislatore ad affrontare nuove problematiche inerenti ai dati diffusi, attraverso strumenti informatici e non solo. Esse richiedevano dal legislatore comunitario una risposta, ossia una regolamentazione unica, che disciplinasse tutele e diritti in tutti i paesi dell'Unione, al fine di creare un'unica disciplina giuridica in tema di trattamento dei dati: **Il Regolamento UE 679/2016**, che troverà applicazione obbligatoria dal 2018 in tutti gli stati membri dell'Unione, costituisce tale importante strumento. Tra le novità più rilevanti? L'ampliamento della tutela in capo all'interessato, ossia il soggetto cui si riferiscono i dati trattati, la definizione del concetto di misure tecniche ed organizzative adeguate che sono volte a mettere in pratica con efficacia i principi di protezione dei dati; Il Regolamento, inoltre, introduce la metodologia della valutazione preventiva d'impatto e la gestione del rischio e delle correlate misure di sicurezza; definisce i nuovi ruoli aziendali connessi alla protezione dei dati personali: "data controller" ossia l'attuale "titolare" e "data processor" ossia l'attuale "responsabile" ed "incaricato". La nuova normativa in materia protezione dati mira ad adeguare la data protection rispetto all'evoluzione tecnologica che ha determinato un aumento dei flussi transfrontalieri e, quindi, dei dati scambiati tra attori pubblici e privati, rendendo così necessari: da un lato, una più libera circolazione di dati all'interno dell'UE ma, dall'altro, un più elevato livello di protezione. Si elimina anche, così, la frammentazione applicativa della normativa in materia di protezione dei dati personali nel territorio dell'UE, dovuta alle diverse leggi di recepimento della Direttiva 95/46, a maggior beneficio dell'incremento degli scambi e dello sviluppo delle imprese e dell'economia.*

La società Sogert è pienamente consapevole, pertanto, nell'adottare il presente SISTEMA DI GESTIONE DELLA PRIVACY degli impegni e degli obiettivi del nuovo Regolamento Europeo 679/2016.

1.0 FONTI NORMATIVE

1.1 Regolamento UE 679/2016



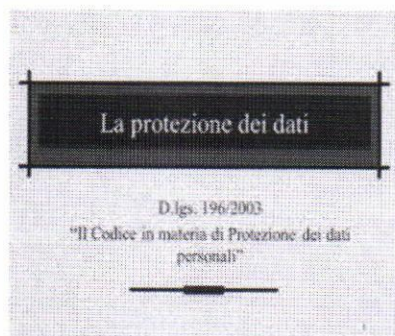
Il Regolamento porterà significative innovazioni non solo per i cittadini, ma anche per le aziende, gli enti pubblici, le associazioni, i liberi professionisti

completamente operativo e vincolante a partire dal 2018.

E'una normativa che contribuisce alla realizzazione di uno spazio di libertà, sicurezza e giustizia, unico, proprio nella Comunità Europea; è una disciplina volta al progresso economico e sociale. Il Regolamento UE 679/2016, come si legge dal dettato normativo: *“mira ad armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati ed assicurare la libera circolazione dei dati personali tra Stati membri. Esso si è reso necessario vista la rapidità dell'evoluzione tecnologica e la globalizzazione, che comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che*

li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione, nonché il loro trasferimento verso paesi terzi e le organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali."

1.2 Codice della privacy 196/2003



Il Codice della privacy, introdotto con decreto legislativo 30 giugno 2003, n.196, innovato nel tempo da altre disposizioni di leggi e regolamenti in materia, rappresenta la disciplina nazionale in materia di protezione dei dati personali e si pone come punto terminale di un lungo e travagliato percorso di adeguamento dell'ordinamento giuridico italiano alle moderne esigenze di protezione dei dati personali. Tale testo in materia di privacy si compone di ben 186 articoli e definisce il diritto alla protezione dei dati personali come un vero e proprio diritto della persona: l'art. 1, infatti, prevede espressamente che "Chiunque ha diritto alla protezione dei dati personali". In tal modo, così come i tradizionali diritti della personalità (nome, immagine, riservatezza), anche il diritto di ogni soggetto, sia esso persona fisica o giuridica, alla protezione dei dati personali viene ad essere tutelato direttamente dalla legge. Con l'introduzione del Nuovo Regolamento comunitario, suddetto Codice, secondo una parte significativa della dottrina, sarà destinato, però, a svolgere un

ruolo sussidiario di applicazione, solo in mancanza di puntuali previsioni contenute nella fonte primaria comunitaria.

1.3 Termini e definizioni del Regolamento EU 679/2016.

- 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico, cartaceo o elettronico-digitale;

- 6) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 7) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; “incaricato”: la persona fisica che coadiuva il responsabile nell'attività;
- 8) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
- 9) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- 10) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- 11) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- 12) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; (4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT 22).



si presenta

2.0 Aspetti generali

SO.GE.R.T. SPA , nel panorama dei progetti per la gestione dei tributi locali, coordina il servizio di tesoreria per Comuni e Consorzi; è, pertanto, una società specializzata nell'attività di riscossione, liquidazione, accertamento, comprese le fasi coattive, delle entrate tributarie ed extratributarie, incluse le sanzioni a qualsiasi titolo emesse, di spettanza degli Enti locali ai sensi dell'art. 52 del D. Lgs. 15 dicembre 1997 n. 446. L'azienda, inoltre, è inserita nell'elenco delle Imprese con Rating di Legalità così come previsto dall'art. 8 del Regolamento adottato dall'Autorità Garante della Concorrenza e del Mercato.

In particolare le sue attività comprendono:

- Accertamento di tutti i tributi per conto degli enti locali (Comuni, Consorzi ecc.)
- Riscossione dell'Imposta comunale sugli immobili (ICI), della Tassa Rifiuti Solidi Urbani (TARSU) e della Tariffa Igiene Ambientale (TIA) per conto dei Comuni
- Riscossione ed accertamento imu
- Riscossione ed accertamento TARI/TARES/TASI
- Riscossione acqua, acque reflue, depurazione ed eccedenza
- Riscossione dei tributi per conto dei Consorzi di bonifica
- Riscossione delle sanzioni per violazioni al Codice della strada
- Riscossione coattiva a mezzo ingiunzione fiscale secondo le procedure disciplinate dal R.D. n.639/1910
- Fase esecutiva secondo il Titolo II D.P.R. 602 del 29 settembre del 1973
- Fornitura di servizi connessi alla riscossione locale (servizi WEB, prodotti informatici, etc.)

- Attività e servizi in favore degli Enti locali (riscossione, rendicontazione incassi, acquisizione ottica, etc.)
- Essere presenti sul territorio con sportello per permettere ai contribuenti di eseguire i versamenti con modalità e forme ispirate al principio della comodità e della economicità
- Servizio di Tesoreria complesso di operazioni relative alla gestione finanziaria dell'Ente, finalizzate alla riscossione delle entrate, al pagamento delle spese, alla custodia dei titoli e valori ed a tutti gli adempimenti previsti dalla legge, dallo statuto, dai regolamenti dell'Ente
- Trasferimento ed archiviazione con firma digitale di mandati e reversali
- Modalità riscossione coattiva:
 - Emissione e notifica delle ingiunzioni di pagamento e/o intimazioni con calcolo di quote aggiuntive (interessi, spese, etc.)
 - Emissione di uno o più solleciti di pagamento
 - Aggiornamento dati anagrafici dei contribuenti con predisposizione e monitoraggio di elenchi nominativi con interrogazioni alle Banche Dati Disponibili (Anagrafe Comunale, Agenzia delle Entrate, Camera di Commercio, Agenzia del Territorio, PRA, etc.)
 - Analisi e valutazione delle possidenze del contribuente
 - Gestione del contenzioso nel rispetto delle attuali normative nelle fasi delle singole procedure cautelative ed esecutive (fermi amministrativi, ipoteche legali, pignoramenti mobiliari, immobiliari, presso terzi, concorsuali)

SO.GE.R.T.SPA è una società per azioni con sede legale in Piazza Domenico Cirillo 5, Grumo Nevano. Le sedi operative sono, invece, circa 24, anche se, alcune di queste, non sono riportate sul sito Internet della Società.

SO.GE.R.T.SPA si avvale di personale altamente qualificato, grazie alla vasta esperienza maturata in anni di attività. Alle dipendenze della società lavorano, attualmente, circa 76 risorse, che svolgono, principalmente, attività di riscossione presso gli sportelli dell'azienda. Si tratta di una organizzazione di risorse che si muovono, lavorano, nel rispetto delle normative tecniche generali e

specifiche nei vari settori sopra menzionati, nel rispetto dei contratti collettivi, e nel rispetto delle norme che regolano la dignità dell'individuo nelle sfere in cui si sviluppa la sua personalità e nelle sue relazioni e nel rispetto delle disposizioni sulla sicurezza e prevenzione dagli infortuni



AREE DI LAVORO

• Sede Centrale

P.zza Domenico Cirillo 5, 80028 Grumo Nevano (NA)

Tel/Fax: 081/5050898

E-mail:

sogert.presidente@libero.it

sogert.areasalegale@pec.it

sogert.presidente@pec.it

Presidente SOGERT s.p.a.: Dott. Felice Coppola

- **Area accertamento:** Dott. Vincenzo Spena - Tel/Fax 081.192.40.824
- **Area amministrativa:** Dott. Renato Chiacchio - Tel/Fax 0823.76.60.04
- **Area gestione tesoreria e tributi:** Francesco Frattolillo - Tel/Fax 081.836.94.15
- **Area legale e commerciale:** Dott. Vincenzo Liguori - Tel/Fax 081.503.09.08
- **Area Pignoramenti/Procedure esecutive:** Olga Coppola - Tel/Fax 081.505.08.98 - pec:sogert.pignoramenti@pec.it - email:sogert.pignoramenti@libero.it
- **Area rapporti con Enti:** Giuseppe Coppola - 081.835.24.32
- **Area riscossione e Contenzioso Enti:** Olga Coppola - Tel/Fax 081.731.35.76
- **Area tecnica economica:** Salvatore Colucci - 081.81.96.336- 081.71.164.53/ 347.80.32.299

2.1 DATA PROTECTION IN AZIENDA

L'azienda ha posto in essere un'articolata policy aziendale ed una serie di misure organizzative e tecniche, mirate alla tutela dei dati personali, per garantire il rispetto della direttiva europea che ha emanato il Nuovo Regolamento UE.

L'azienda SO.GE.R.T.SPA, in quanto titolare del trattamento, si è attivata per elevare il grado di sicurezza dei dati delle persone fisiche già prima che lo stesso Regolamento Comunitario sia vincolante (maggio 2018), assicurando la massima trasparenza, attuando misure organizzative e tecniche e, ancora, progettando, ad esempio, le modalità di custodia dei dati, predisponendo misure al fine di evitare la distruzione, perdita e diffusione degli stessi.

Ottemperando alle prescrizioni del Legislatore comunitario, il titolare del trattamento ha predisposto nuove informative, redatte secondo le nuove indicazioni della normativa comunitaria, che contiene i dati di contatto, la tipologia dei dati personali trattati, le finalità del trattamento, l'indicazione dei termini entro i quali si prevede l'eliminazione dei dati, l'indicazione dei legittimi interessati, eventuale ambito di trasferimento dei dati ad un'organizzazione internazionale o fuori dall'Ue.

2.2 IL REGISTRO DEI TRATTAMENTO

Con il presente Registro, SO.GE.R.T.SPA , definisce gli indirizzi e le principali procedure di sicurezza in materia di protezione dei dati personali, nonché i criteri tecnico-organizzativi per la loro attuazione. Descrive le regole e gli obiettivi del SGP (sistema di gestione privacy), i documenti di riferimento relativi alle diverse fasi di implementazione, attuazione e monitoraggio del Sistema, le responsabilità e i compiti dei soggetti coinvolti. Fornisce altresì, idonee informazioni relative alla tipologia dei dati personali trattati, nonché i possibili rischi e impatti sui dati degli interessati. Il Registro delle attività di trattamento non deve essere visto solo come un adempimento, bensì come uno strumento utile a mappare, in maniera ordinata e precisa, strumenti e metodi operativi, come i DataBase e le misure di protezione utilizzate nel processo di trattamento oltretutto a costituire il più importante documento atto a provare che il Titolare del Trattamento ha adempiuto al dettato normativo previsto dal nuovo Regolamento in materia di Privacy. Il registro è un documento di gestione della privacy all'interno dell'azienda, importante, perché rappresenta la gestione fedele dei trattamenti che avvengono sui dati secondo la prescrizione del Regolamento UE 679/2016. Esso contiene, inoltre, le seguenti informazioni: il nome e i dati di contatto del titolare del trattamento, il nome e dati di contatto del Responsabile protezione dati (DPO), il nome e i dati del responsabile/incaricato del trattamento (interno/esterno); il nome e i dati dell'amministratore, le modalità e finalità del trattamento; le categorie di interessati e le categorie di dati personali, e le misure minime che si vogliono adottare. Esso viene depositato ed è disponibile presso la sede legale della Società.

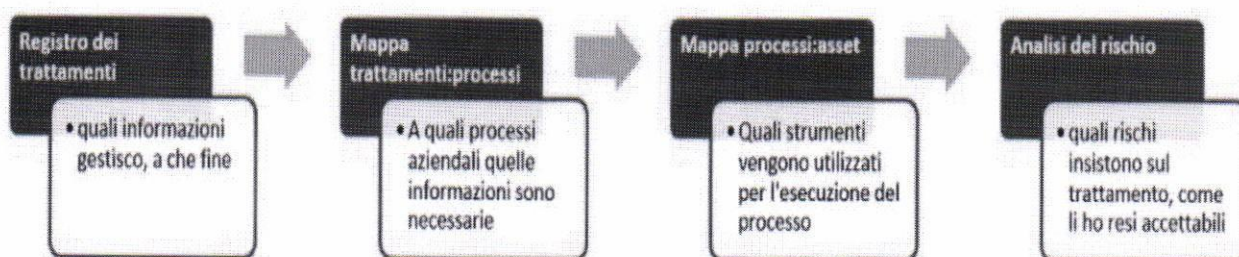
3.0 METODOLOGIA PER ANALISI DEI RISCHI PER SO.GE.R.T.SPA

3.1. PREMESSA

A seguito delle interviste effettuate ai personali preposti ai vari processi è stata effettuata una ricognizione dei trattamenti che ha tenuto conto dei principi dettati dall'art.5 del GDPR 2016/679 e che hanno sottoposto all'attenzione del titolare dell'azienda : la tutela dei dati personali , le garanzie di tutela, l'adeguatezza delle misure di protezione, la liceità del trattamento, l'esistenza delle misure tecniche ed organizzative adeguate per evitare la perdita, la distruzione anche accidentale dei dati, misure finalizzate all'integrità e sicurezza dei dati.

Informazioni generali sul trattamento dei dati personali

Informazioni generali sul trattamento dei dati personali



3.2 Asset

Per ciascun trattamento (o, appunto, categoria di trattamento) sono state raccolte informazioni

Interviste: Asset circa:

1. la natura, la finalità e il contesto del trattamento (incluse le fonti presso cui i dati vengono raccolti, l'estensione del trattamento, il coinvolgimento di terze parti all'interno o al di fuori del territorio europeo, e così via),
2. le categorie di dati (personali e sensibili) oggetto di trattamento, i soggetti interessati a cui si riferiscono e il periodo di conservazione dei dati,
3. i flussi informativi (ipotesi di comunicazione, diffusione, cessione, trasferimento dei dati con l'indicazione specifica dei soggetti destinatari dei dati interni o esterni all'organizzazione del titolare del trattamento),
4. una descrizione funzionale delle operazioni di trattamento,
5. le modalità (cartacee e automatizzate) e gli strumenti con cui viene effettuato il trattamento (comprehensive dell'impiego di tecnologie, tra cui ad esempio *hardware* e *software*, e dell'indicazione dei canali e dei *network* attraverso cui passano i dati),
6. i soggetti che potranno accedere ai dati unitamente alle finalità o alle motivazioni sottese all'access, ecc.

3.3 Pre-assessment e Risk-assessment

Una volta individuate le aree più a rischio (vedi l'allegato RISCK ASSESSMENT-DETTAGLIO FRAMEWORK NAZIONALI DI CYBER SECURITY) quali le infrastrutture tecnologiche e applicazioni IT di SO.GE.R.T.SPA, è stata fatta una valutazione, **Pre -assessment**, delle loro capacità di contenere il rischio e solo dopo l'analisi del rischio **Risk-assessment** e i gap emersi si è potuto stimare il livello di impatto che l'eventuale accadimento dell'evento potesse avere sull'Ente.

Con quest'ultima analisi si è proceduto di volta in volta ad elaborare delle **misure tecniche ed organizzative** al fine di eliminare/limitare l'impatto, ad esempio Sogert ha già da tempo adottato la certificazione **ISO 27001**, che sottopone l'azienda ad un continuo monitoraggio e riesame di tutti gli aspetti concernenti la sicurezza delle informazioni aziendali, dalla perdita di dati agli accessi non autorizzati, agli attacchi virus, consentendo attraverso questo sistema di gestione della sicurezza informatica di valutare attentamente tutti i rischi per le diverse tipologie di informazioni gestite, evidenziando le aree in cui è necessario un miglioramento.

SO.GE.R.T.SPA ha adempito ai dettati normative in tema di accountability, valutando il rischio prima che il trattamento abbia inizio (Garanzie by design e by default), misure organizzative (es: policy, istruzioni, formazione, procedure che disciplinano l'aspetto organizzativo); misure di sicurezze fisiche (es: misure di protezione di aree, apparecchiature, dati); misure di sicurezza logiche (es: backup, piano di continuità operativa, piano di disaster recovery, ecc.) sia in relazione al corretto utilizzo degli strumenti elettronici, sia in relazione alla loro gestione e manutenzione.

4.0 MODALITA' DI TRATTAMENTO DEI DATI IN SO.GE.R.T. SPA



4.1 Tipologia di trattamento

La fase preliminare di analisi ed interviste condotta in azienda, e la conseguente fase di elaborazione e aggregazione, hanno portato alla individuazione e classificazione delle seguenti tipologie di dati trattati:

TIPOLOGIA di dati

1. Dati personali relativi ai dipendenti

- ☐ Cognome e nome
- ☐ Stato civile
- ☐ Luogo e data di nascita
- ☐ Domicilio e/o residenza
- ☐ Codice fiscale
- ☐ Numero di telefono
- ☐ Anzianità di inoccupazione certificata (all'atto dell'assunzione)
- ☐ Numero di matricola assegnato
- ☐ Anzianità di servizio
- ☐ N. di posizione I.N.A.I.L.
- ☐ Numero e tipologia dei conviventi fiscalmente a carico (con eventuale quota percentuale)
- ☐ Redditi da precedenti rapporti di lavoro tenuti nel corso dell'anno solare
- ☐ Redditi da lavoro conseguiti in anni precedenti
- ☐ Titolo di studio – formazione ricevuta
- ☐ Indirizzo ip
- ☐ Userid ePw
- ☐ L'immagine

2. Dati personali particolari (sensibili) relativi ai dipendenti

- ☐ Infortuni
- ☐ Invalidità
- ☐ Esposizioni a fattori di rischio
- ☐ Idoneità psico-fisica a svolgere determinate mansioni
- ☐ Appartenenza a determinate categorie protette
- ☐ Certificazione sanitaria (no diagnosi) attestante lo stato di malattia
- ☐ Documentazione relativa alla sorveglianza sanitaria dei lavoratori, consegnata dal medico competente nel rispetto del D. Lgs. 196/2003 e della salvaguardia del segreto professionale, nel caso di cessazione dell'incarico (art. 25, comma 1, lettera "d", D. Lgs. 81/08)
- ☐ Cartella sanitaria (art. 25, comma 1, lettera "c"), consegnata dal medico competente nel rispetto del D. Lgs. 196/03 e della salvaguardia del segreto professionale, nel caso di cessazione del rapporto di lavoro del dipendente (art. 25, comma 1, lettera "e", D. Lgs. 81/08)
- ☐ Dati anonimi collettivi comunicati dal medico competente in corrispondenza della sorveglianza sanitaria (art. 25, comma 1, lettera "i", D. Lgs. 81/08) dei lavoratori
- ☐ Dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere politico o sindacale
- ☐ Procedimenti disciplinari
- ☐ Dati relativi a cessione del 5° dello stipendio

3. Dati relativi all'utenza

- ☐ Cognome e nome
- ☐ Stato civile
- ☐ Luogo e data di nascita
- ☐ Domicilio e/o residenza
- ☐ Codice fiscale
- ☐ Numero di telefono
- ☐ Matricola

Tali dati sono trattati con strumenti elettronici e cartacei.

Per la gestione dei dati, il Titolare del trattamento ha definito, nel presente registro, le categorie di interessati e le responsabilità, ha definito informative che, alla presente, si allegano nei confronti dei dipendenti, e dell'utenza, ha previsto nomine a coloro i quali, di fatto, trattano dati e ne hanno la responsabilità, ha prescritto indicazioni ai Responsabili ed agli Incaricati per osservare quanto richiesto dal Regolamento UE.

Inoltre, nel presente Registro, vengono prescritte le condotte, che si desumono anche dagli atti di nomina, che devono tenere i responsabili esterni del trattamento, gli incaricati al trattamento che si interfacciano con il titolare del trattamento, i quali devono adempiere alle istruzioni e misure tecniche ed organizzative messe in campo da SO.GE.R.T.SPA, e che opportunamente dovranno interagire con il titolare e con il Data protection officer istituito.

Tutti i soggetti nominati al trattamento sono stati edotti sulle procedure da seguire quando si presentano dei danni ai dati, a seguito di attacchi informatici, come ad esempio l'opportunità immediata di mettersi in contatto con l'Autorità di Controllo, entro le 72 ore, ma prima ancora informare il titolare del trattamento e il data protection officer dell'avvenuta violazione.

Nel Registro, vi è presente l'Organigramma delle Responsabilità, dove vengono indicati i vari Responsabili del trattamento, il Data protection officer, L'amministratore di sistema ed Incaricati. Questi sono nominati con un apposito atto, nel quale dovrà essere inserito il tempo per l'espletamento dell'incarico, il tipo di trattamento e l'area di competenza, le istruzioni finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento.

Vediamo nello specifico le modalità di trattamento dei dati di SO.GE.R.T.



a) Trattamenti dei dati non automatizzati

I soggetti designati quali responsabili o incaricati al trattamento devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.

Gli atti e i documenti contenenti dati personali identificativi e particolari, sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione, in maniera che, ad essi, non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati particolari dove l'accesso agli archivi è controllato (ad es. porta chiusa a chiave, armadio chiuso, ecc.); le chiavi sono in possesso dell'incaricato dell'ufficio preposto, che si occuperà anche di verificare che le persone che accedono ai locali siano quelle autorizzate. Le persone ammesse, a qualunque titolo, (ad es. gli addetti alle pulizie) sono identificate preventivamente autorizzate e soprattutto istruite. La documentazione cartacea risulta localizzata e organizzata come di seguito descritto:

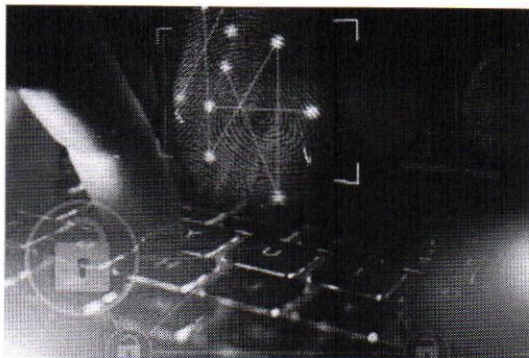
- ✓ i dati personali identificativi e quelli particolari relativi al personale dipendente, curricula, qualunque dato che lo identifichi, sono custoditi in armadi e/o cassettiere chiusi a chiave o in locali dotati di porta di accesso con chiusura a chiave (area risorse umane);
- ✓ i dati relativi a fornitori (che identificano la persona fisica) della Società sono custoditi nell'apposito ufficio di pertinenza chiuso a chiave (area risorse umane).

4.2 Prescrizioni

SO.GE.R.T.SPA, prescrive le seguenti condotte che sono già oggetto di una attività di comunicazione a tutti coloro che di fatto gestiscono i dati.

Pertanto l'azienda ha disposto che dipendenti adeguatamente istruiti devono organizzare e localizzare la documentazione cartacea come di seguito descritta:

- ✓ È necessario che, dopo il trattamento, i documenti e i faldoni siano riposti in archivi chiusi a chiave, eventualmente in un cassetto chiuso a chiave, e/o una cassaforte, e/o un armadio blindato. La stanza dove sono depositati i dati deve essere chiusa a chiave.
- ✓ È necessario avere particolare cura per i dati particolari (dati sensibili), quei dati personali idonei a rivelare l'origine razziale ed etnica di una persona, le sue convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare il suo stato di salute e la vita sessuale; ci si deve, in particolare, assicurare che un visitatore o terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) non possa venire a conoscenza dei contenuti di tali documenti;
- ✓ eventuali fotocopie non riuscite bene devono essere distrutte in un apposito distruggitore, se disponibile, oppure devono essere strappate in pezzi talmente piccoli da non consentire in alcun modo la ricostruzione del contenuto, che deve essere in ogni caso illeggibile.



b) Trattamenti automatizzati

Il trattamento dei dati delle persone fisiche avviene anche con strumenti informatici. Si tratta di dati personali riguardante il personale ma anche e soprattutto l'utenza comunicata dalle'Ente Territoriale, per la riscossione dei tributi, e per l'accertamento degli stessi . In particolare le aree di trattamento sono Area accertamento, Area amministrativa, Area gestione tesoreria e tributi, Area legale e commerciale, Area Pignoramenti/Procedure esecutive, Area riscossione e Contenzioso Enti, Area tecnica economica.

Il trattamento dei dati avviene tramite un sistema computerizzato, i cui pc sono collegati ad un Server di proprietà della SO.GE.R.T affidato in gestione a So.te.i. srl (la società che si occupa delle soluzioni e delle tecnologie informatiche), che gira su piattaforma IBM, si tratta del gestionale per la riscossione dei tributi per conto dei comuni. Un altro software gestionale utilizzato è fornito dalla società Dedagroup s.p.a. con il quale è possibile caricare i file relativi alla procedura di accertamento messa in atto da SO.GE.R.T.SPA, in quanto ricostruisce tutti i dati del contribuente.

I principali pacchetti software utilizzati permettono la gestione **dei dati relativi alla riscossione di tributi (ordinaria, coattiva e pignoramenti)** per conto dei comuni nonché la trasmissione delle

informazioni e la gestione delle notifiche ai contribuenti tramite un ente esterno INTEGRA (stampa imbusta e consegna gli atti).

In particolari i software:

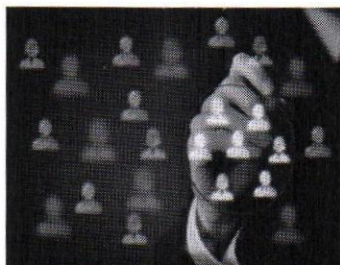
- 1) Procedure varie in fogli Excel (macro)
- 2) Client Access IBM collegati ad AS400 (gestione riscossione)
- 3) Software gestione ACCERTAMENTI
- 4) Software gestione TESORERIA
- 5) Applicativi web

L'accesso in particolare al Client Access IBM avviene tramite autenticazione con *username* e *password* abilitati e con profili creati da SOTEL in accordo con l'amministratore dr. Frattolillo. Tali applicativi risiedono sui Server e questo garantisce una sicurezza in termine di backup e salvaguardia dei dati. Vengono anche effettuati aggiornamenti fornite dalle case produttrici direttamente sui servers e distribuite automaticamente alle applicazioni Clients. Norme ulteriori a salvaguardia dei dati e configurazioni sono:

- 1) La gestione delle credenziali di accesso utente con cambio di password a cadenza trimestrale e verifica dei permessi
- 2) La gestione degli aggiornamenti software e delle licenze d'uso con verifica di tutti i software installati
- 3) La gestione degli accessi ad Internet e alla posta elettronica. In questo caso oltre alle protezioni firewall , antivirus e antispam dovrebbe essere prevista anche l'installazione futura di un **server proxy** che possa regolamentare in qualche modo anche la navigazione web.

In merito al backup per la salvaguardia dei dati non sono presenti unità NAS in sede, ma tutti i dati vengono copiati all'interno del Server AS400 che dispone di vari dischi in RAID e inviati al Server farm esterno in Germania.

5.0 DALL'ANALISI DEI RISCHI ALLE MISURE TECNICHE ED ORGANIZZATIVE



Premessa

Dall'analisi dei rischi condotta da Sogert, come riportato **nell'allegato dal titolo RISK ASSESSMENT** che fa riferimento al Framework Nazionale di Cyber Security elaborato dal CIS (Università La Sapienza di Roma), l'azienda è intervenuta potenziando le aree tecnico -informatiche, dandosi un'organizzazione strutturale delineando compiti e responsabilità, elaborando policy secondo il nuovo regolamento eu, L'azienda ha rilevato la necessità di nominare un Data protection officer, che potesse fungere da punto di contatto con le Autorità di Controllo, e soprattutto ha acquisito la consapevolezza dell'importanza della formazione e di fornire istruzioni ai propri dipendenti sui comportamenti da tenere nell'utilizzo dei dati.

Rafforzando le sicurezza logica, fisica ed organizzativa ha adempiuto alle raccomandazioni del legislatore europeo.

5.1 Struttura organizzativa

SO.GE.R.T.SPA , ha individuato ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del sistema di sicurezza, con riferimento alla tutela dei dati sia delle persone fisiche all'interno dell'azienda e sia delle persone fisiche con cui vengono a contatto.

L'articolazione organizzativa prevede:

- Un **Data protection Officer**, punto di contatto con l'Autorità di Controllo e l'azienda SO.GE.R.T., la sua responsabilità principale sarà quella di osservare, valutare ed organizzare la gestione del trattamento di dati personali e dunque la loro protezione, affinché questi dati siano trattati nel rispetto delle norme privacy europee e nazionali.
- l'**Amministratore di sistema e di rete** con il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione, cui competono la gestione delle risorse di calcolo centrali, i collegamenti in rete all'interno ed all'esterno della struttura, nonché la cura, l'installazione e lo sviluppo delle stesse, nonché l'assistenza agli utenti per l'accesso alle risorse ed alla rete. L'amministratore ha inoltre competenza in materia di sicurezza su ogni risorsa di calcolo comunque afferente alla propria struttura nel cui ambito è individuato almeno un referente per il *Computer Security Incident Response Team* (CSIRT);
- **Responsabili del trattamento esterno**, soggetti che trattano dati per conto dell'azienda e che sono tenute a rispettare le istruzioni, le misure tecniche ed organizzative, impartite dal titolare del trattamento.
- **Incaricati del trattamento**, ossia i soggetti che trattano i dati in azienda, definizione che non compare nel Nuovo Regolamento Data Protection, ma si preferisce utilizzare per identificare e nominare i soggetti che trattano i dati.

5.2 I SOGGETTI DELLA PRIVACY: DETERMINAZIONE DEI COMPITI

Dal punto di vista organizzativo l'azienda SO.GE.R.T.SPA, seguendo il dettato normativo in particolare l'art.24 del GDPR (accountability) ha provveduto a strutturare la propria organizzazione, ponendo così in essere quelle **misure organizzative** necessarie al fine prevenire rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, ha definito il presente registro, ha definito un organigramma privacy, ha implementato delle policy e delle procedure.

5.3 ORGANIZZAZIONE e RUOLI

Ha definito un **ORGANIGRAMMA** dove vengono definiti chiaramente i RUOLI e le RESPONSABILITÀ in materia di Privacy, Sicurezza e Controllo;

SO.GE.R.T.SPA, si è dotato di un organigramma privacy che prevede il titolare del trattamento, responsabili del trattamento, incaricati del trattamento, amministratore di sistema e Data protection officer.

Andiamo nello specifico:



Titolare

Ex art 5 e 26 del Regolamento eu è la persona, fisica o giuridica, nel nostro caso, l'azienda SO.GE.R.T che – singolarmente o insieme ad altri - determina finalità e mezzi del trattamento e adotta misure tecniche e organizzative per garantire e dimostrare che il trattamento sia effettuato in conformità al Regolamento; è sempre il Titolare, qualora ve ne sia la necessità, a definire le politiche da adottare in materia di protezione dei dati personali.



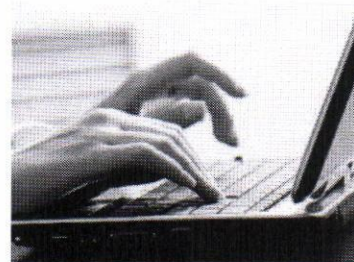
Responsabile/i

Ex art.4 e 28 del Regolamento eu è la persona fisica o giuridica che, a seguito di una designazione formale, effettua il trattamento di dati personali per conto del Titolare.

In particolare il Titolare, prima di designare un Responsabile del trattamento e di affidargli l'incarico, deve verificarne le caratteristiche e le competenze professionali, ed assicurarsi che offra garanzie sufficienti (misure tecniche e organizzative) ed adeguate, finalizzate a tutelare i diritti degli interessati. I trattamenti effettuati dal Responsabile del trattamento devono essere disciplinati da una nomina che vincoli il Titolare e lo stesso Responsabile del trattamento. Nell'accordo il titolare dovrà inserire il tipo di dati che tratta il Responsabile, in particolare dovrà contenere una descrizione dettagliata delle attività da svolgere – tipologia dei dati personali trattati, finalità e durata del trattamento, obblighi e diritti del titolare – e dovrà prevedere che il Responsabile possa effettuare le attività di trattamento esclusivamente dietro istruzione documentata del Titolare, soprattutto in caso di trasferimento dei dati personali verso un'organizzazione internazionale o un paese terzo. Il Responsabile dovrà garantire, altresì, che le persone autorizzate a trattare i dati personali, all'interno della propria struttura, si siano impegnate alla riservatezza. Il responsabile del trattamento dovrà mostrare garanzie, nel momento in cui si affida nell'espletamento di un servizio in cui è interessato un trattamento di dati a Sub-Responsabili. Tali garanzie, afferiscono sempre alle misure tecniche ed organizzative imposte dal titolare, in presenza delle quali lo stesso titolare potrà autorizzare alla successiva nomina. In sintesi il Responsabile qualora volesse affidare il trattamento dei dati ad un servizio esterno sarà necessaria sempre un atto di nomina, un contratto, atto giuridico, da parte del Responsabile al Sub-Responsabile, debitamente autorizzato dal titolare del trattamento.

In sintesi i principali compiti condivisi con il titolare

- ✓ valutare i rischi inerenti al trattamento nell'ambito della Policy aziendale,
- ✓ attuare misure per limitare i rischi;
- ✓ valutare il rischio ogni volta che inizia un nuovo trattamento dei dati dovuto (ad esempio: perdita accidentale dei dati, accessi non autorizzati);
- ✓ modalità e durata di conservazione dei dati.
- ✓ Predisporre un programma formativo
- ✓ Individuare le categorie di dati a rischio ecc.



Incaricati del trattamento

regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4).

Per opportuna di maggiore tutela, il SO.GE.R.T ha nominato incaricati al trattamento, in sintesi l'incaricato è colui che effettua materialmente le operazioni di trattamento sui dati personali. **Può essere solo una persona fisica, e deve agire sotto la diretta autorità del titolare del trattamento.** Questo ci indica che se in teoria è possibile che un incaricato sia un soggetto esterno all'azienda, nella pratica risulterebbe difficile. La normativa impone che la semplice presa visione di un dato personale si qualifica come trattamento, e quindi necessita di un formale incarico perché non sia considerato illecito. Ugualmente, non rileva la circostanza che l'incarico sia a pagamento o gratuito, e nemmeno se il collaboratore è esterno (es. il lavoratore chiamato a riparare il computer che,

ovviamente, può accedere ai dati ivi contenuti) invece che inquadrato nell'azienda.

E' fondamentale tenere presente che in assenza della nomina di incaricati, qualsiasi operazione svolta dai dipendenti o collaboratori del titolare non sarà qualificata come un utilizzo interno dei dati, bensì come una comunicazione a terzi con tutte una serie di problematiche che ne derivano, l'Autorità di controllo italiana ha precisato che la mancata designazione degli incaricati è una violazione dell'obbligo di applicazione delle misure minime di sicurezza. che sono quei dipendenti che lavorano nell' organizzazione e che coadiuvano il Responsabile del trattamento.

In sintesi I compiti:

- ✓ adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'Incaricato;
- ✓ custodire in modo diligente i dispositivi, in possesso ed uso esclusivo, con i quali possono accedere ad uno o più strumenti informatici;
- ✓ tenere sotto chiave gli archivi di cui hanno la gestione;
- ✓ non lasciare incustoditi sulle scrivanie, faldoni, documenti, ecc.

Amministratore di Sistema

E'una figura professionale che approfondisce le competenze di un tecnico hardware e software soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, i livelli di sistemistica e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione. i occupa quindi essenzialmente di ogni tipo di rete informatica, comprese quelle a cui non si accede via web, come le reti intranet e, non per ultimo implementa i sistemi di sicurezza del networking nonché definisce le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte

gli utenti, curando interventi di conservazione dei dati attraverso debite soluzioni di “backup” e progettando le attività di supporto al “disaster recovery”. L’amministratore di sistema durante l’espletamento dei suoi incarichi, pur se meramente tecnici, ha un considerevole impatto di responsabilità sui dati aziendali. A lui spetta il compito di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento UE 27 aprile 2016 n.679).E’ la persona che dovrebbe rendersi conto di un eventuale violazione o perdita dei dati, accidentale od intenzionale che sia, è proprio l’amministratore di sistema che, con la sua attività quotidiana, svolge routine di sicurezza informatica volte a garanzia della struttura informatica. Il tema della sicurezza informatica non si esaurisce, dunque, solo con semplici installazioni di prodotti antivirus, regole di networking e policy stringenti ma soprattutto con costanti monitoraggi proattivi della rete e delle sue componenti che, ovviamente, devono essere attuati da personale altamente specializzato, ora più che mai viste anche le pesanti sanzioni poste a carico dei titolari del trattamento in caso di inosservanza.

In sintesi I compiti:

- ✓ assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda;
- ✓ predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- ✓ predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di “amministratore di sistema”); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
- ✓ custodia dei supporti nei quali sono stati memorizzati i dati;
- ✓ adottare misure finalizzate alla protezione del sistema da virus informatici o intrusioni non autorizzate nella propria rete informatica (programmi antivirus, firewall) ecc.

- ✓ pianificare gli aggiornamenti software per correggere i difetti dei programmi o dei sistemi operativi utilizzati;
- ✓ controllare che per l'installazione del software sui sistemi o pc aziendali, la Società (o il cliente, quando si lavori presso o per questo) possieda la licenza;
- ✓ controllare che non venga installata alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza sua espressa autorizzazione.

Data protection officer

Si ritiene necessario la nomina di tale figura alla luce dell'analisi dei rischi effettuata la nomina del DPO, in quanto l'azienda tratta dati su vasta scala. Un **Data protection Officer**, rappresenta il punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. La sua responsabilità principale sarà quella di osservare, valutare ed organizzare la gestione del trattamento di dati personali e dunque la loro protezione, affinché questi dati siano trattati nel rispetto delle norme privacy europee e nazionali.

Il Regolamento non fornisce una definizione di "trattamento su larga scala", anche se il considerando 91 fornisce indicazioni in proposito, ricomprendendovi, in particolare, "trattamenti che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

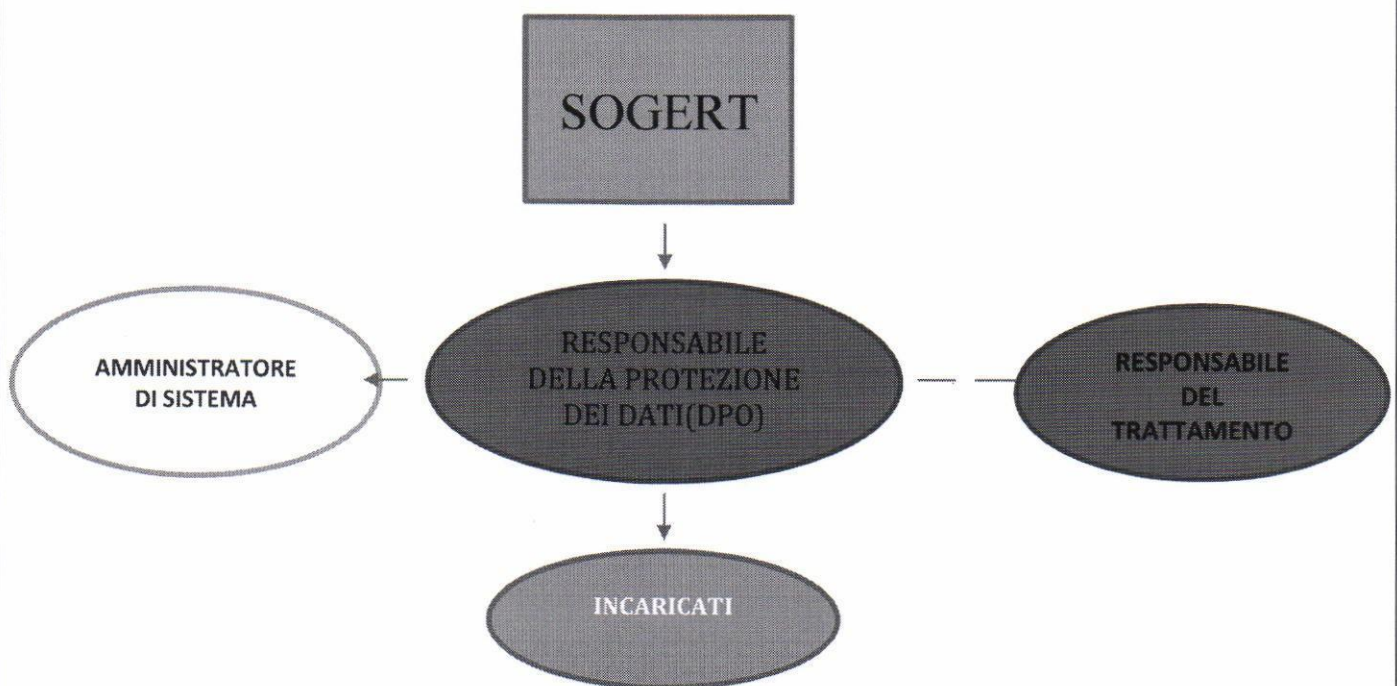
Le linee guida evidenziano come fra tali estremi si colloca un'ampia zona grigia e che in realtà risulta impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità.

Ad ogni modo, il Working Party raccomanda di tenere conto, in particolare, dei seguenti fattori:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Nel rispetto di quanto previsto dall'art. 37 del GDPR, il DPO, DATA PROTECTIO OFFICER è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

- a) informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD (nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati);
- b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
- d) cooperare con il Garante per la protezione dei dati personali



5.4 Organigramma delle Responsabilità

Dati personali /dp

Dati personali particolari/dpp

Titolare del trattamento è



Sede Legale Piazza Domenico Cirillo 5 - Grumo Nevano (NA)

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Trattamento interno ed esterno	Descrizione degli strumenti utilizzati	Resp.tratt.
		dpp	dp				
Finalità perseguita o attività svolta	Categorie di interessati						
Coordinamento e monitoraggio dei trattamenti dei dati Coordinamento funzionale dei Responsabili del trattamento	Personale dipendente, Clienti e Fornitori, utenza altrii interessati	x	X	Amministrazione	Tratt. interno	PC collegati in LAN, Internet	TITOLARE DEL TRATTAMENTO SO.GE.R.T.SPA ,
Gestione attività amministrativa, legale, accertamenti , riscossione, risorse umane, area tecnica economica, pignoramenti e procedure esecutive, gestione tesoreria e tributi	Personale dipendente	x		Risorse umane	Trattamento automatizzato e non	Computer aziendali	Incaricati del trattamento (Vedi lista)
Attività di supporto e consulenza	Figura di contatto			società		Computer	DPO RESPONSABILE DELLA PROTEZIONE DATI
Medicina di sorveglianza (Idoneità, patologie ecc.)	Personale dipendente	X	X	Risorse Umane	Tratt.esterno	Computer propri	Responsabile esterno (medico competente) Augusto Lombardi
Buste paga, previdenza, contributi, attestazioni pagamento assenze giustificate a qualsiasi titolo.	Buste paga dipendenti	X	X	Contabilità/Risorse umane	Tratt.esterno	Computer propri	Responsabile Esterno La Comara Maurizio
Banche dati	utenza		X	Gestione dati	Tratt.esterno	Computer propri	Responsabile Esterno SO.TE. I

Consulenza fiscale e contabile	utenza	x	x	Fiscale e contabile Risorse umane/società	Tratt.esterno	Computer propri	Responsabile Esterno D'Aponte Carmine
Servizi di formazione	utenza		x	Servizi di consulenza	Tratt.esterno	Computer propri	Responsabile ESTERNO B&P CONSULTING srl
Servizi di sicurezza sul lavoro	utenza		x	Servizi di consulenza	Tratt.esterno	Computer propri	Responsabile ESTERNO SARDELLA CONSULENZE SRL
Servizi IT	utenza		x	Servizi di consulenza	Tratt.esterno	Computer propri	Responsabile ESTERNO DEDA GROUP SPA
Servizi	utenza		x	Servizi di consulenza	Tratt.esterno	Computer propri	Responsabile ESTERNO HALLEY CAMPANIA
Servizi di posta privata	utenza		x	Gestione posta	Trattamento esterno	Computer propri	Responsabile ESTERNO POSTA INTEGRA
Dati utenza del web	Utenza		x	Dati web	Trattamento dati sito web, gestione archivio informatizzato	Archivio Informatico	Incaricato del sito web Renato Chiacchio
L'Amministratore di sistema IT	Dipendenti, clienti, fornitori.	x	x	Sicurezza informatica	Area It	PC collegati in Lan, Internet	Amministratore di sistema Francesco Frattolillo

5.4 AREA TECNOLOGICA: Sito web, videosorveglianza, posta elettronica

a) SITO WEB

Il sito presentava delle lacune di tipo informativo, per le quali si è provveduto a colmarle, inserendo un banner iniziale che porta la seguente dicitura “ ” Utilizziamo i cookie per migliorare la vostra esperienza di navigazione. Continuando a navigare nel sito si accetta la nostra PRIVACY POLICY DEL SITO WEB ed Utilizzo dei cookie”.

PRESCRIZIONI che ha eseguito

Policy chiare sull'utilizzo dei dati raccolti dall'utenza ed informative sull'utilizzo dei cookie.

b) VIDEOSORVEGLIANZA



Presso la sede Legale e le sedi operative saranno presenti strumenti di videosorveglianza, di cui saranno stati edotti i dipendenti con idonee informative e l'utenza con cartellonistica ben visibile.

Tali telecamere rispetteranno i requisiti richiesti dalla novellata normativa legge:

Statuto dei lavoratori Legge 20 maggio 1970, n. 300 art. 4 comma 1 che recita:

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di

imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della **sede centrale dell'Ispettorato nazionale del lavoro.**

Le immagini registrate dalla società dagli strumenti di videosorveglianza saranno salvate per 5 giorni, dopodiché, grazie alla presenza di un disco sovrascrivibile, si annullano.

PRESCRIZIONI

Il datore di lavoro come indicato dal Garante con (Prov. Garante Privacy 8 aprile 2010) deve:

- informare i lavoratori con appositi cartelli della presenza delle telecamere;
- nominare un incaricato della gestione dei dati videoripresi;
- posizionare le telecamere verso le zone a rischio, evitando di collocarle in maniera unidirezionale sui lavoratori impegnati nella loro attività;
- conservare le immagini raccolte solo per un arco temporale consentito dalla legge e salvo esigenze speciali.



c) POSTA ELETTRONICA

La posta aziendale costituisce uno strumento di lavoro e il dipendente a cui viene riservato uno specifico indirizzo e-mail, è tenuto ad utilizzarlo esclusivamente per motivi organizzativi e lavorativi. Al fine di assicurare il rispetto dei diritti della privacy nell'ambito delle finalità dello strumento di posta elettronica, la società fornisce opportune informazioni e disposizioni circa il corretto utilizzo della stessa, attraverso i normali canali di comunicazione aziendale (comunicati, informative, formazioni ecc.)

6.0 VERIFICHE DELL'ADEGUATEZZA DELLE MISURE

Uno dei compiti che Sogert si è data è di verificare periodicamente l'adeguatezza ed efficacia delle misure adottate provvedendo ad adeguare le stesse alla particolare evoluzione tecnologica del settore, al fine di mantenere elevato il livello di protezione e ridurre, quindi, il livello di rischio. L'attività di verifica verrà attuata mediante procedure di **monitoraggio** e di **audit** ed in particolare:

- attraverso un sistema di **monitoraggio** effettuato da responsabili interni che eseguono un controllo costante dell'effettivo funzionamento del sistema informatico e delle misure di sicurezza, adottando tutte le misure necessarie ad incrementarne il livello di efficacia;
- attraverso la previsione di un'attività di **audit**, quale controllo saltuario svolto da soggetti *diversi* dai responsabili interni, al fine di ottenere un giudizio imparziale circa la qualità delle misure di sicurezza approntate ed in grado di evidenziarne eventuali debolezze od errori.



Il Titolare del Trattamento pianifica e attua i processi di monitoraggio, analisi, valutazione, verifica e miglioramento del Sistema di Gestione per la Privacy (SGP) finalizzati a:

- ✦ garantire e dimostrare la conformità del SGP ai requisiti previsti dal presente documento ed ai requisiti cogenti applicabili;
- ✦ valutare le prestazioni e l'efficacia del SGP;
- ✦ migliorare in modo continuo le performance e l'efficacia del SGP, provvedendo a conservare appropriate informazioni documentate come evidenza dei risultati delle attività svolte.

Gli audit interni sono uno strumento efficace per determinare i livelli di conformità del SGP rispetto a criteri stabiliti, identificare problematiche, rischi e non conformità, fornire informazioni utili per analizzare e migliorare in continuo le prestazioni del sistema, promuovere buone prassi all'interno dell'Organizzazione.

SOGERT S.p.a. definisce il processo di gestione degli audit interni, e si interfacerà con il DPO, documentando le responsabilità e i requisiti per la pianificazione, la conduzione e la registrazione dei risultati, in coerenza con quanto previsto nella relativa procedura gestionale del SGQ.

Ciascun audit si conclude con la predisposizione di un apposito rapporto, nel quale sono riepilogati gli esiti delle verifiche svolte.

Il risultato degli Audit è importante perché consente al Data protection Officer, (Responsabile della protezione dei dati) congiuntamente al Titolare, di valutare le opportunità per il miglioramento continuo delle misure organizzative e tecniche adottate. Il processo di miglioramento segue un approccio strutturato secondo la metodologia PDCA, in coerenza con quanto previsto dal SGQ.

7.0 DATI DI CONTATTO

1) TITOLARE DEL TRATTAMENTO DEI DATI

COGN. _____ NOME _____

NATO A _____, IL _____

RESIDENTE A _____

IN VIA _____ Tel/cell _____

2) RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO)

COGN. _____ NOME _____

NATO A _____, IL _____

RESIDENTE A _____

IN VIA _____ Tel/cell. _____

2.1) -RESPONSABILI ESTERNO DEL TRATTAMENTO DEI DATI

AZIENDA SO.GE.R.T. S.P.A.

COGN. COPPOLA NOME GIUSEPPE

NATO A NAPOLI, IL 12/12/1979

RESIDENTE A GRUMO NEVANO (NA)

IN VIA CASSO P. EZZ D. CIRILLO N° 5 Tel/cell. _____

2.2) RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

AZIENDA

COGN. FRATTOLILLO NOME FRANCESCO

NATO A CAIVANO (NA), IL 01/03/1964

RESIDENTE A CAIVANO (NA)

IN VIA CATALANI, 2 Tel/cell _____

2.3) RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

AZIENDA

COGN. _____ NOME _____

NATO A _____, IL _____

RESIDENTE A _____

IN VIA _____ Tel/cell _____

3) AMMINISTRATORE DI SISTEMA

COGN. FRATTOLILLO NOME FRANCESCO

NATO A CAIVANO (NA), IL 01/03/1964

RESIDENTE A CAIVANO (NA)

IN VIA CATALANI, 2 Tel/cell. _____

4) INCARICATO DEL TRATTAMENTO DEL SITO WEB

COGN. CHIACCHIO NOME RENATO MARIA

NATO A NAPOLI, IL 8/01/1983

RESIDENTE A NAPOLI

IN VIA MANZONI 314 P Tel/cell _____

7.1 ELENCO INCARICATI

NOME

COGNOME

AREA
BANCA DATI/UFFICIO

FRANCESCO	FRATTOLILLO	

