SCARANOFUSCA INVESTMENT S.R.L.
Via Dogana, 3 – Milano (20123 – MI)
C.F. / P.I. 12082290961

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

INTRODUZIONE ALLA PARTE SPECIALE

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2011	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 - 20123 Milano P. IVA – C. F. 12082290961

INDICE

Introduzione alla Parte Speciale

La Parte Speciale del Modello definisce i principi generali e speciali di comportamento (Protocolli) ed i criteri per la definizione delle regole di organizzazione, gestione e controllo (Procedure) che devono guidare la Società e tutti i Destinatari del Modello nello svolgimento delle attività nell'ambito delle quali possono essere commessi i Reati Presupposto.

La Parte Speciale si compone di otto sezioni, ciascuna dedicata ad una categoria di Reati Presupposto considerati rilevanti per la Società.

In particolare, alla luce del contesto socio economico in cui opera la Società, della sua storia e della tipologia delle attività svolte, la stessa ha ritenuto potenzialmente rilevanti le seguenti categorie di Reati Presupposto:

- **Parte Speciale *A*** - Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto) nonché induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies* del Decreto);

- **Parte Speciale *B*** - Delitti informatici e trattamento illecito di dati (artt. 24 e 24 *bis* del Decreto), nonché Delitti in materia di violazione del diritto d'autore (Art. 25 *novies* del Decreto);

- **Parte Speciale *C* -** Delitti di criminalità organizzata (art. 24 *ter* del Decreto);

- **Parte Speciale *D*** – Delitti contro la fede pubblica (Art. 25 *bis* del Decreto) e reati contro l'industria ed il commercio (Art. 25 *bis.1* del Decreto);

- **Parte Speciale *E*** - Reati Societari (art. 25 *ter* del Decreto) e Reati di Ricettazione e riciclaggio nonché autoriciclaggio (art. 25 *octies* del Decreto);

- **Parte Speciale *F* -** Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 *septies* del Decreto);

- **Parte Speciale *G*** - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies* del Decreto – introdotto con il D.Lgs 109/2012);

- **Parte Speciale *H*** - Reati tributari (art. 25 *quinquiesdecies* del Decreto – introdotto con D.L. 124/2019, convertito con modificazioni dalla L.157/2019);

Ciascuna sezione della Parte Speciale: ***a)*** individua preliminarmente le cosiddette **aree di attività "sensibili"**, vale a dire quelle aree, ovvero funzioni aziendali, nell'ambito delle quali vengono svolte le attività per cui è astrattamente possibile la commissione di uno dei Reato Presupposto esaminati, quindi ***b)*** indica i **principi generali** di comportamento che devono informare l'attività dei Destinatari del Modello che operano nell'ambito delle suddette aree sensibili e ***c)*** indica **principi specifici** di comportamento e le procedure di

prevenzione adottatedalla Società.

I principi di controllo applicabili alle attività sensibili preventivamente individuate sono stati definiti utilizzando come riferimento le *best practice* internazionali di categoria, tenendo indebita considerazione le procedure implementate in ambito aziendale.

I principi di controllo, il cui rispetto risulta necessario ai sensi del presente Modello per poter prevenire la commissione di qualsiasi Reato Presupposto sono:

- **segregazione delle attività**: deve esistere una forma di segregazione delle attività tra chi esegue, chi controlla e chi autorizza;

- **norme/circolari**: devono esistere disposizioni aziendali idonee a fornire almeno i principi di riferimento generali per la regolamentazione dell'attività;

- **poteri di firma e poteri autorizzativi**: qualora l'Amministratore Unico decida di conferire deleghe di funzioni dovranno esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi;

- **tracciabilità**: il soggetto che firma le comunicazioni scritte alla pubblica amministrazione deve assicurare la tracciabilità delle relative fonti e degli elementi informativi.

Tutti i destinatari del Modello sono chiamati ad osservare, ai fini della sua corretta applicazione, quanto di seguito indicato.

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "A"

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 – 20123 Milano P. IVA – C. F. 12082290961

INDICE

1. La nozione di pubblica amministrazione

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti che la Società Scaranofusca Investment S.r.l. instaura con la Pubblica Amministrazione.

Con l'espressione "Pubblica Amministrazione" si intende quel complesso di Autorità, di organi e di agenti cui l'ordinamento affida la cura degli interessi pubblici che vengono individuati:

- nelle **istituzioni pubbliche locali, regionali, nazionali, comunitarie e internazionali** intese come strutture organizzative aventi il compito di perseguire con strumenti giuridici, gli interessi della collettività; tale funzione pubblica qualifica l'attività svolta anche dai membri della Commissione delle Comunità Europee, del Parlamento Europeo, della Corte di Giustizia e della Corte dei Conti delle Comunità Europee;

- nei **pubblici ufficiali**, intesi come persone fisiche che, a prescindere da un rapporto di dipendenza dello Stato o da altro ente pubblico esercitano una funzione pubblica legislativa, giudiziaria o amministrativa; per pubblica funzione "amministrativa", si intende una funzione disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi (art. 357, co. 2 c.p.).

- negli **incaricati di pubbliche funzioni o servizi** che svolgono un'attività riconosciuta come funzionale ad uno specifico interesse pubblico e disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, quanto al contenuto, dalla mancanza dei poteri autoritativi e certificativi propri della pubblica funzione, con la quale è solo in rapporto di accessorietà o complementarietà.

Qualora, nello svolgimento della propria attività, dovessero sorgere problematiche interpretative sulla qualifica (pubblica o privata) dell'interlocutore, ciascuno dei Destinatari del presente Modello dovrà rivolgersi all'Organismo di Vigilanza al fine di richiedere gli opportuni chiarimenti.

2. Reati contro la pubblica amministrazione

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati di cui agli articoli 24 e 25 nonché all'articolo 25 *decies* del D.Lgs. 231/2001, i quali vanno contemplati anche tenendo conto delle fattispecie del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

3. Identificazione delle aree di rischio e delle attività sensibili

La mappatura delle attività sensibili e, quindi, a rischio reato, ha consentito di individuare, non solo le attività c.d. sensibili in senso stretto, ma anche una serie di "attività strumentali", dalle quali potrebbe astrattamente derivare la commissione di uno dei reati presupposto di cui alla presente Parte Speciale.

Sono **attività sensibili** in senso stretto quelle che presentano rischi diretti di rilevanza

penale in relazione ai Reati Presupposto individuati dal Decreto.

Le **attività strumentali**, invece, si identificano con quelle attività che, pur non presentando rischi diretti di rilevanza penale, se combinate con le attività direttamente sensibili, possono supportare la realizzazione del reato costituendone la condotta illecita.

Il rischio di commissione dei reati presupposto, trattati nella presente parte speciale, riguarda nello specifico quelle funzioni e quelle attività che implicano la costituzione di rapporti giuridici con la Pubblica Amministrazione nella gestione tipica di ogni processo produttivo.

La configurazione dei reati presupposto di cui alla presente Parte Speciale, per quanto non si possa escludere, in ogni caso, è ragionevolmente prevenuta attraverso il rispetto dei principi etici e delle regole comportamentali enunciate nel presente Modello e nel Codice Etico adottati dalla Società.

3.1 Funzioni coinvolte

Di seguito si evidenziano, in macroaree, le Funzioni/Direzioni aziendali responsabili per la Società di eseguire e monitorare le attività sensibili:

- Amministratore Unico
- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

3.2 Attività sensibili

Tali funzioni aziendali sono competenti per quanto attiene a:

- **Gestione dei rapporti con la PA, anche in occasione di visite e verifiche ispettive**
  - Rapporti con le Amministrazioni, ovvero enti pubblici e società pubbliche (es., Autorità, Enti Pubblici territoriali, Stazioni Appaltanti, Amministrazioni) Committenti, e gestione dei relativi rapporti con le medesime amministrazioni coinvolte;
  - Gestione dei rapporti con gli enti previdenziali ed assistenziali, (es. INPS, INAIL, Cassa Edile, Fondi Previdenza Complementare), i Centri per l'impiego, il Ministero del Lavoro e delle Politiche sociali e i Sindacati;
  - Gestione dei rapporti con la P.A., con i suoi consulenti tecnici ed ausiliari, nell'ambito del contenzioso (civile, penale, amministrativo e tributario);
  - Gestione dei rapporti con gli organi competenti/funzionari pubblici in caso verifiche ed ispezioni (es. ispezioni da parte dell'amministrazione finanziaria, Agenzia delle Entrate, Guardia di Finanza, Autorità di Pubblica Sicurezza in genere, verifica del rispetto delle condizioni richieste dalla legge per assunzioni categorie protette).
- **Gestione dei rapporti con la PA per adempimenti**

- Predisposizione ed invio dichiarazioni ad Enti pubblici per pagamento imposte e contributi (es. adempimenti fiscali ed amministrativi cui l'azienda è tenuta per legge);
- Adempimenti nei confronti di Enti previdenziali e assistenziali, Centri per l'impiego, Ministero del Lavoro e delle Politiche sociali, Sindacati, etc.

- **Gestione dei contenziosi giudiziali e stragiudiziali (es. civili, tributari, amministrativi, penali, etc.), nomina dei legali e coordinamento delle loro attività**
  - Gestione transazione e conciliazioni con le Autorità Pubbliche di riferimento;
  - Gestione dei contenziosi giudiziali e stragiudiziali, nomina dei legali e coordinamento delle loro attività (selezione consulenti legali e certificazione servizi).
- **Ciclo passivo**
  - Selezione dei Consulenti esterni;
  - Selezione dei consulenti ed intermediari per incarichi professionali riguardo la Gestione Risorse Umane;
  - Selezione, negoziazione e stipula di contratti con fornitori/subappaltatori;
  - Ricezione beni/Certificazioni dei servizi;
  - Ricezione beni/Certificazione servizio (relativamente a prestazioni professionali di consulenti fiscali / amministrativi / legali);
- **Gestione degli approvvigionamenti ed attività correlate**
  - selezione fornitori;
  - gestione dei flussi finanziari – monetari in uscita;
- **Assunzione, gestione, formazione del personale e incentivazione anche con riferimento al personale appartenente alle categorie**
- **Gestione dei flussi e delle transazioni finanziarie**
- **Gestione omaggi e liberalità**
- **Gestione spese di rappresentanza e di trasferta**
- **Gestione delle sponsorizzazioni**

4. Protocolli comportamentali e procedure di prevenzione

Ai fini dell'attuazione delle regole comportamentali e dei divieti elencati nei paragrafi successivi, i Destinatari della presente Parte Speciale del Modello, oltre a rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale, devono rispettare i protocolli comportamentali di seguito descritti, posti a presidio dei rischi reato sopra identificati (artt. 24 e 25 nonché 25 *decies* del D. Lgs. 231/2001) e riferibili alle attività sensibili e alle procedure di

prevenzione indicate.

4.1 Principi generali di comportamento

Tutti i Destinatari del presente Modello, come individuati nella Parte Generale, adottano regole di comportamento conformi ai principi di seguito elencati nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle aree di attività sensibili e strumentali indicate nel paragrafo 3 (3.1 e 3.2), al fine di prevenire il verificarsi dei reati contro la Pubblica Amministrazione rilevanti per la Società e previsti dal Decreto.

Costituiscono presupposto e parte integrante dei principi generali di comportamento di cui al presente paragrafo, dei principi specifici e dei criteri per la definizione dei protocolli di prevenzione di cui al paragrafo successivo, i principi individuati nel Codice Etico della Società, ivi da intendersi integralmente richiamati.

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Parte Speciale sono oggetto di segnalazione all'OdV da parte di tutti i dipendenti e degli organi sociali, ed in generale da parte di tutti i Destinatari.

In generale, **è fatto espresso divieto** a tutti i Destinatari del Modello di:

- intrattenere rapporti con la Pubblica Amministrazione, in rappresentanza o per conto della Società, **in mancanza di apposita delega e/o procura**, appositamente conferita dall'Amministratore Unico in forma scritta;

- utilizzare, nella gestione dei rapporti con la Pubblica Amministrazione, eventuali percorsi preferenziali o conoscenze personali, anche acquisite al di fuori della propria realtà professionale, al fine di influenzarne le decisioni;

- offrire denaro o altre utilità a Pubblici Ufficiali o incaricati di Pubblico Servizio o ancora a organi o funzionari dell'Autorità Giudiziaria, inclusi i familiari degli stessi, al fine di influenzarne la loro discrezionalità, l'indipendenza di giudizio o per indurli ad assicurare un qualsiasi vantaggio alla Società;

- riconoscere, in favore di fornitori o collaboratori esterni, o loro familiari che operano in diretto contatto con la Pubblica Amministrazione, in nome e per conto della Società, compensi indebiti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;

- corrispondere e/o proporre la corresponsione e/o chiedere a terzi di proporre la corresponsione di denaro o altre utilità a un Pubblico funzionario dell'Autorità Giudiziaria o a suoi familiari, nel caso in cui la Società sia parte di un procedimento giudiziario;

- intraprendere attività economiche, conferire incarichi professionali, dare o promettere doni, danaro, o altri vantaggi ad Autorità Pubbliche che effettuino accertamenti e ispezioni, ovvero ad organi dell'Autorità Giudiziaria;

- ricorrere a forme di contribuzioni che, sotto veste di sponsorizzazioni, incarichi,

consulenze, pubblicità, configurino, invece, forme di doni o regalie verso pubblici funzionari, loro familiari, ovvero enti e autorità pubbliche, ovvero a società ricollegabili all'area pubblica;

- presentare dichiarazioni, comunicazioni o documenti contenenti informazioni non veritiere, fuorvianti o parziali alla Pubblica Amministrazione, ovvero omettere informazioni, al fine di ottenere provvedimenti favorevoli dalla Pubblica Amministrazione;

- destinare a finalità diverse da quelle per le quali sono stati eventualmente concessi contributi, sovvenzioni o finanziamenti o altre erogazioni dello stesso tipo, ottenuti dallo Stato o da altro ente pubblico o dall'Unione Europea.

I Destinatari della presente Parte Speciale del Modello devono astenersi dal porsi in situazioni di possibile conflitto di interessi e, nel caso in cui ciò avvenga, ne devono dare immediata comunicazione al superiore gerarchico e all'OdV.

La Società Scaranofusca Investment S.r.l. fa espresso divieto di perseguire interessi e/o vantaggi per la Società tramite la realizzazione di condotte illecite le quali, come tali, non trovano in nessun caso giustificazione a livello aziendale.

4.2 Principi specifici di comportamento e procedure di prevenzione e controllo dei rischi sottostanti alla conduzione delle attività strumentali

Per tutte le operazioni relative alle attività sensibili individuate nel precedente paragrafo 3.2 è in linea di massima individuato un Responsabile Interno nel procedimento per l'attuazione di dette operazioni.

Salvo diversa indicazione, il Responsabile Interno del procedimento si identifica con il Responsabile della Funzione/Direzione competente per la gestione dell'operazione considerata.

Quando vi sono più Direzioni coinvolte nella gestione della medesima operazione il Responsabile Interno del procedimento si identifica con il Responsabile della Direzione che intrattiene in modo più diretto e costante rapporti con la Pubblica Amministrazione.

Il Responsabile Interno del procedimento è responsabile dell'operazione a rischio e deve garantire il rispetto delle regole di condotta, delle politiche e delle procedure aziendali che attengono, in particolare, ai rapporti tra la propria Direzione e la Pubblica Amministrazione.

Tutte le operazioni relative alle attività sensibili individuate al precedente paragrafo 3.2 sono regolamentate, tra l'altro, dalle seguenti procedure di prevenzione e controllo:

- ogni operazione e/o transazione aziendale deve essere autorizzata dall'Amministratore Unico, documentata, motivata, registrata e riscontrabile in ogni momento;

- alle ispezioni o alle verifiche amministrative partecipa il responsabile della Funzione/Direzione, o dell'ufficio oggetto di ispezione, e/o i soggetti da

quest'ultimo espressamente delegati per iscritto, **unitamente ad altro dipendente della medesima Direzione interessata**;

- il Responsabile della Funzione/Direzione, o dell'ufficio oggetto di verifica di ispezione, informa l'Amministratore Unico (ed eventualmente in casi di particolare rilevanza l'OdV) dell'inizio del procedimento;

- **in caso di addebiti eventualmente mossi alla Società, il medesimo Responsabile di Funzione/Direzione informa prontamente i citati organi di quanto rilevato in sede di ispezione inoltrando idoneo *report***;

- nel caso in cui non venga mossa alcuna contestazione e/o rilievo alla Società, i Responsabili formalizzano un *report* interno, **con cadenza almeno annuale**, da inviare alla Direzione competente, oltre che all'Amministratore Unico, relativo alle ispezioni verificatesi;

- tutti gli atti, i contratti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione, devono essere gestite e sottoscritte solo da coloro che sono dotati di idonei poteri di rappresentanza della società;

- è vietato disporre il pagamento in contanti, di qualsivoglia natura, oltre la soglia consentita dalla legislazione vigente;

- l'accesso ai documenti già archiviati deve essere sempre consentito solo alle persone autorizzate, all'Amministratore Unico, e all'Organismo di Vigilanza;

- la scelta dei consulenti esterni incaricati della gestione del contenzioso avviene esclusivamente in base ai requisiti di professionalità, indipendenza e competenza. L'incarico è conferito per iscritto con indicazione del compenso pattuito o dei criteri per determinarlo, nonché del contenuto della prestazione fornita;

- occorre garantire la correttezza e veridicità della documentazione predisposta dalla Società ed inviata all'Autorità Regolatoria;

- **i contratti prevedono apposite clausole che richiamano le responsabilità derivanti dal D. Lgs. 231/2001 ed il rispetto del presente Modello**.

I principi specifici di comportamento e le procedure di prevenzione, descritti *ut supra,* devono essere rispettati in relazione a tutte le attività, o le operazioni aventi ad oggetto i rapporti con qualsiasi organo e/o ente della P.A.

Per tutte le operazioni legate alle c.d. "attività strumentali", come identificate nel precedente paragrafo 3.2:

- la Funzione/Direzione competente verifica periodicamente a lista dei soggetti muniti di deleghe a porre in essere operazioni bancarie e comunica eventuali modifiche e/o aggiornamenti alle banche presso cui la Società ha aperto i propri conti correnti bancari;

- gli acquisti di servizi sono motivati ed effettuati previo esperimento di una procedura competitiva informale che consenta di selezionare l'offerta migliore, valutata sulla base di criteri oggettivi, imparziali e trasparenti predeterminati. Sono fatte salve le ipotesi di selezione diretta in caso di necessità di ottenere l'esecuzione di prestazioni di particolare complessità, ovvero in casi di urgenza, sempre previa autorizzazione del competente superiore gerarchico;

- i compensi corrisposti ai fornitori, oltre che ai consulenti, devono essere conformi r congrui al servizio della Società in considerazione delle condizioni di mercato o delle eventuali tariffe professionali vigenti per la categoria di appartenenza;

- la documentazione afferente alla prestazione del servizio (*i.e.* i contratti, la modulistica, evidenze della prestazione, etc.) viene conservata e archiviata a cure della Direzione competente;

- la Società vieta espressamente di promettere o offrire ai pubblici ufficiali, ovvero incaricati di pubblico servizio (o a loro parenti, affini o parti correlate) denaro, doni o omaggi (superiori al limite **di euro 50,00**) salvo che si tratti di doni o utilità d'uso di modico valore (ad es. non sono di modico valore viaggi e soggiorni, pagamento di quote di iscrizione a circoli, etc.);

- le liberalità di carattere benefico o culturale devono rientrare nei limiti previsti dalle norme vigenti e nel pieno rispetto delle stesse, oltre che in linea con i principi enunciati nel Codice Etico e nel Modello medesimo;

- è fatto divieto di promettere o concedere ai soggetti esercenti una pubblica funzione (o a loro parenti, affini o parti correlate) opportunità di assunzione e/o opportunità commerciali (o di qualsiasi altro genere) privi di una giustificazione, che quindi siano posti in essere solo per avvantaggiarli a livello personale;

- la richiesta di nuove assunzioni deve essere motivata ed autorizzata dall'Amministratore Unico;

- nel processo di assunzione del personale sono individuati criteri oggettivi per la valutazione dei candidati (ad es. voto di laurea, precedenti esperienze professionali) che rispondono ad esigenze di trasparenza nel processo di selezione del candidato;

- è vietato favorire nei processi d'acquisto fornitori e sub-fornitori segnalati da pubblici ufficiali che condizionino a tale preferenza lo svolgimento successivo delle attività a cui i medesimi fornitori e sub-fornitori sono incaricati;

- le proposte di impiego di risorse finanziarie per sponsorizzazioni devono essere documentate dalla Funzione/Direzione proponente, la quale deve indicare espressamente i destinatari, le ragioni e l'importo concesso.

Le Funzioni/Direzioni interessate, l'Amministratore Unico, i singoli dipendenti, oltre che l'OdV propongono, ove ne emerga la necessità, le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

5. Flussi informativi nei confronti dell'OdV

Allo scopo di consentire all'Organismo di Vigilanza di monitorare e verificare in modo tempestivo l'effettiva esecuzione dei controlli previsti dal presente Modello e, in particolare, dalla presente Parte Speciale, nelle procedure sono descritti i flussi informativi che devono essere assicurati al predetto Organismo in conformità a quanto disposto nella Parte Generale del Modello stesso.

Come visto, devono essere formalizzati da parte del Responsabile Interno adeguati reports periodici, **con cadenza almeno annuale** (salvo il verificarsi di eventi straordinari) indirizzati all'Amministratore Unico e all'OdV, che documentino le attività rilevanti poste in essere nell'ambito della gestione delle relazioni con le Pubbliche Autorità (es. eventuali addebiti mossi dalla P.A.).

L'OdV potrà richiedere alle Direzioni competenti, anche a campione, la documentazione di supporto relativa alle operazioni poste in essere nell'ambito delle "attività sensibili e strumentali".

Le Direzioni/Funzioni Aziendali coinvolte garantiscono, coordinando le strutture di propria competenza, la documentabilità del singolo processo monitorato, comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento critico cui sono legati i rischio-reato.

Lo strumento di comunicazione è rappresentato prevalentemente dalla e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it, con la specificazione nell'oggetto del reference del flusso informativo cui si riferisce la comunicazione medesima.

SCARANOFUSCA INVESTMENT S.R.L.
Via Dogana, 3 – Milano (20123 – MI)
C.F. / P.I. 12082290961

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "B"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI NONCHE'REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 – 20123 Milano P. IVA – C. F. 12082290961

INDICE

Introduzione

L'art. 24 *bis* del D. Lgs. 231/01 ha introdotto l'obbligo, per gli enti, di definire precise norme comportamentali e direttive di controllo, nei processi di gestione ed utilizzo dei sistemi informatici aziendali, al fine di prevenire la possibile commissione di delitti informatici, nonché un illecito trattamento dei dati in possesso dell'ente.

Deve evidenziarsi che il Legislatore con la novella del 2000, intervenendo in materia di tutela del software (art. 171 bis, L. 633/1991), ha modificato il profilo soggettivo del delitto in esame, sostituendo il fine di lucro con il mero fine di profitto.

In altri termini, oggi, non sono sanzionati solo i comportamenti finalizzati ad ottenere, dalla illecita duplicazione di *software*, un guadagno di tipo prettamente economico, ma anche le ipotesi della duplicazione di un *software* finalizzata a risparmiare il costo del programma originale e della relativa licenza d'uso.

Per tale ragione, tutte le aziende che usano, a scopi lavorativi, dei programmi non originali, senza avere la relativa licenza d'uso, anche al solo fine di risparmiare il costo del software originale, saranno passibili di responsabilità *ex* art. 25 *novies* del decreto legislativo n. 231/01.

Limitatamente allo svolgimento delle attività sensibili alle quali essi eventualmente partecipano, possono essere destinatari di specifici obblighi, strumentali ad un'adeguata esecuzione delle attività di controllo interno previste nella presente Parte Speciale, i seguenti soggetti esterni (nel prosieguo anche solo "Soggetti Esterni"):

- i collaboratori, i consulenti e, in generale, i soggetti che svolgono attività di lavoro autonomo nella misura in cui essi operano nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società;

- i fornitori e i partner (in qualsiasi forma societaria o associativa) che operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società.

Tra i Soggetti Esterni, così definiti, debbono ricondursi anche coloro che, sebbene abbiano in corso rapporti contrattuali con altra società, nella sostanza operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società.

La Società Scaranofusca Investment S.r.l. ha applicato misure di sicurezza in grado di proteggere efficacemente il sistema informatico e, quindi, prevenire la commissione dei reati informatici.

In ogni caso, la presente Parte Speciale del Modello ha, quale obiettivo, quello di indirizzare, mediante regole di condotta, le attività sensibili poste in essere dai Destinatari **al fine di prevenire il verificarsi dei delitti informatici e di trattamento illecito dei dati di cui all'art. 24 *bis* del Decreto 231/2001, nonché dei delitti in materia di violazione del diritto d'autore di cui all'art. 25 *novies* del medesimo Decreto**.

Nello specifico, essa ho lo scopo di:

- illustrare le fattispecie di reato riconducibili agli artt. 24 *bis* e 25 *novies* del Decreto;
- identificare le attività sensibili, ossia quelle attività che la Società pone in essere ed in relazione alle quali, secondo un approccio di *risk assesment*, appare possibile la configurazione dei reati presupposto richiamati dal Decreto agli artt. 24 *bis* e 25 *novies*;
- riprendere e specificare i principi generali e specifici di comportamento del Modello;
- illustrare i protocolli comportamentali, implementati dalla Società al fine di prevenire i rischi-reato in esame, che i destinatari sono tenuti ad osservare per una corretta applicazione della presente Parte Speciale del Modello;
- riepilogare i riferimenti alle specifiche *policies* e procedure finalizzate alla prevenzione di rischi-reato in esame;
- fornire, all'Organismo di Vigilanza, gli strumenti operativi per esercitare le necessarie attività di controllo, monitoraggio e verifica nell'adozione del Modello da parte della Società;

1. Rinvio al catalogo dei reati

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati informatici e trattamento illecito dei dati nonché dei delitti in materia di violazione del diritto d'autore di cui agli artt. 24 *bis* e 25 *novies* del d.lgs. 231/2001, i quali vanno contemplati anche tenendo conto delle fattispecie del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

2. Identificazione delle aree di rischio e delle attività sensibili

2.1 Le aree sensibili

Di seguito si evidenziano, in macroaree, le Funzioni/Direzioni aziendali responsabili per la Società di eseguire e monitorare le attività sensibili:

- Amministratore Unico
- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

2.2 Le attività sensibili

Per quanto attiene all'identificazione delle attività sensibili sono state individuate le seguenti areedi attività "sensibili" a rischio:

- **Gestione delle attività di accesso ai sistemi informatici/telematici e applicazioni (autocertificazione, account e profili);**
- **Gestione dell'attività di elaborazione dei dati;**
- **Attività di manutenzione dei sistemi informatici/telematici e di accesso alle applicazioni;**
- **Gestione e manutenzione hardware;**
- **Gestione, sviluppo e manutenzione software;**
- **Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT;**
- **Attività di creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;**
- **Attività di trasmissione dati ed informazioni alle pubbliche autorità;**
- **Gestione della sicurezza informatica.**

3. Principi generali di comportamento

I Destinatari del presente Modello sono tenuti ad osservare i seguenti principi generali:

- occorre tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e delle procedure interne;
- è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dalla presente Parte Speciale.

Con specifico riguardo alle problematiche connesse al rischio informatico, la Società, consapevole dei continui cambiamenti tecnologici e dell'elevato impegno operativo, organizzativo e finanziario necessario ad aggiornare le componenti *hardware* e *software* aziendali, si impegna a mantenere un efficace sistema di sicurezza informatica, in particolare attraverso:

i. la protezione dei sistemi e delle informazioni dai potenziali attacchi, attraverso l'utilizzo di strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attacchi;

ii. la garanzia della massima continuità del servizio.

Sulla base degli standard di riferimento internazionali, per sistema di sicurezza informatica deve intendersi l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali che la Società si pone, nell'ambito della sicurezza informatica, sono:

- **riservatezza**, ossia garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione dei dati stessi, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- **integrità**, ossia garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- **disponibilità**, ossia garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione.

In particolare, coerentemente con il rispetto dei principi deontologici, si determina che:

- i sistemi di autenticazione e di accesso alle risorse informatiche/telematiche devono rispettare i principi di unicità, incedibilità e segretezza;

- i sistemi di autenticazione e di accesso alle strutture fisiche, atte alla conservazione delle risorse informatiche/telematiche, devono rispettare i principi di unicità, incedibilità e segretezza;

- la Società deve promuovere le migliori condizioni di utilizzo, irrobustimento e protezione delle *password* personali di accesso ai sistemi e delle migliori condizioni di utilizzo dei dispositivi elettronici;

- è fatto divieto ai soggetti non autorizzati di accedere ai sistemi informatici/telematici della Società o di terzi;

- è fatto divieto ai soggetti non autorizzati di accedere abusivamente alle strutture fisiche atte alla conservazione delle risorse informatiche/telematiche (es. *server*) della Società;

- è fatto divieto ai soggetti non autorizzati di detenere e diffondere, abusivamente, codici di accesso alle strutture fisiche atte alla conservazione dei sistemi informatici/telematici;

- è obbligatorio, da parte di tutto il personale interno od esterno (utenti), nonché dagli addetti alla predisposizione degli strumenti informatici, il rispetto delle procedure aziendali riguardanti la sicurezza dei sistemi informativi, anche quelle richiamate all'interno dei documenti *privacy* e, in generale, nella normativa aziendale specifica;

- è obbligatorio da parte di tutto il personale, interno od esterno (utenti), segnalare immediatamente al proprio responsabile o alla funzione competente, la presenza di anomalie in materia di sicurezza, non conformità o vulnerabilità, connesse ai sistemi informatici/telematici o alle strutture atte alla loro conservazione;

- è obbligatorio il rispetto delle procedure aziendali per l'approvvigionamento di prodotti e servizi riguardanti i sistemi informatici;

- è fatto divieto di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;

- l'utilizzo dei dispositivi informatici/telematici deve rispettare le *policy* in materia di sicurezza dei sistemi informatici;

- l'utilizzo di c.d. *storage device* (es: memorie USB, CD, DVD, etc) deve rispettare le *policy* in materia di sicurezza dei sistemi informatici;

- l'installazione di dispositivi informatici/telematici *hardware* e *software* deve rispettare la *policy* in materia di sicurezza dei sistemi informatici e, prima ancora, la normativa dettata in tema di *copyright*;

- è fatto divieto di installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;

- è fatto divieto di danneggiare informazioni, dati e programmi informatici;

- ogni utente ha il dovere di usare le stazioni di lavoro e le applicazioni, cui può accedere per i soli scopi ed entro gli esclusivi limiti, anche temporali, inerenti la sua mansione e di evitare che altri possano accedere a tali strumenti di lavoro. A tal fine, la Società adotta le misure di sicurezza previste sia dalle disposizioni di cui sopra sia da quelle adottate in conformità ai requisiti di cui al Codice Privacy e ss.mm.ii;

- in nessun caso, anche qualora disponga di diritti di amministrazione sulla rete, un utente può eseguire prove di penetrazione della rete informatica della Società, anche laddove abbia riscontrato specifiche vulnerabilità. I test di penetrazione della rete informatica (probing) possono essere effettuati dalla Delivery Manager area IT e/o dai soggetti/società esterni, nei limiti di quanto previsto dai relativi contratti di servizio o dalle specifiche utenze di amministratore di sistema. In quest'ultimo caso, la società incaricata deve dare preventiva comunicazione all'Amministratore Unico della natura dell'intervento da effettuare per il tramite delle competenti funzioni aziendali;

- ogni utente deve comunicare al responsabile dell'unità organizzativa cui è assegnato (o al proprio referente, nel caso di utenti esterni) tutte le violazioni rilevate o sospettate inerenti alla sicurezza (in particolare, vigilare sull'uso delle proprie chiavi di accesso ed autenticazione) e provvedere ad inoltrare idonea informativa sia alla funzione che presidia la sicurezza dei sistemi informativi che alla funzione di revisione interna.

È, inoltre, fatto obbligo ai destinatari del presente Modello di attenersi alle seguenti prescrizioni:

- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile diretto, sentito il Responsabile IT;

- in caso di smarrimento o furto delle apparecchiature informatiche, informare tempestivamente il Responsabile diretto e il Responsabile IT, e presentare denuncia all'Autorità preposta;

- evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo siano stati acquisiti con il loro espresso consenso, nonché applicazioni/software che non siano state preventivamente approvate dal Responsabile IT o la cui provenienza sia dubbia;

- evitare di trasferire all'esterno e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà della Società, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del relativo responsabile e del Responsabile IT;

- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC, evitare di consentire l'utilizzo dello stesso a terzi (familiari, amici, etc.);

- evitare l'utilizzo di password di altri utenti;

- utilizzare la connessione ad internet per gli scopi e il tempo strettamente necessari allo svolgimento delle attività che hanno reso indispensabile il collegamento;

- impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla stessa;

- astenersi dall'effettuare copie non specificamente autorizzate di dati e di *software*;

- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;

- osservare scrupolosamente quanto previsto dalle politiche di sicurezza per la protezione e il controllo dei sistemi informatici.

4. Principi specifici di comportamento e procedure di prevenzione

Al fine di dare attuazione alle regole comportamentali e ai divieti elencati nella presente Parte Speciale, i Destinatari della presente sezione del Modello, oltre a dover rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale, devono rispettare i protocolli comportamentali specifici, qui di seguito descritti, posti a presidio dei rischi-reato sopra identificati e riferibili alle attività sensibili, nonché le procedure di prevenzione indicate.

I protocolli comportamentali, pertanto, prevedono obblighi e/o divieti, specifici, che i Destinatari della presente Parte Speciale del Modello devono rispettare, uniformando la propria condotta agli stessi nello svolgimento delle attività sensibili sopra elencate.

Segnatamente, ai Destinatari è fatto divieto di:

- porre in essere, dare causa o comunque contribuire alla realizzazione di comportamenti idonei a configurare le fattispecie di reato richiamate nella presente Parte Speciale;

- dare causa o contribuire alla realizzazione di comportamenti i quali, sebbene non costituiscano di per sé reato, possano potenzialmente configurarlo in futuro.

In particolare, è fatto obbligo:

- al Responsabile IT di denunciare alla Direzione ed all'OdV eventuali accessi al sistema informatico aziendale da parte di *hacker*;

- ai dipendenti, collaboratori, dirigenti, all'Amministratore Unico, di attenersi alle procedure ed istruzioni operative in riferimento all'utilizzo del Sistema Informatico;

- a tutti i Destinatari, di svolgere le attività e le operazioni, per conto della nel rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza.

Si riportano, di seguito, gli standard di controllo "specifici" applicati alle attività sensibili individuate.

Standard di controllo specifici

Disposizioni sulla Sicurezza Informatica
La Società deve adottare una specifica politica in materia di sicurezza del sistema informatico che preveda, fra l'altro:

- le modalità di comunicazione anche a terzi;

- le modalità di riesame della stessa, a cadenza periodica o a seguito di cambiamenti significativi.

Organizzazione della sicurezza per gli utenti interni ed esterni
La Società deve dotarsi di uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso degli utenti interni all'azienda, e gli obblighi cui gli stessi sono tenuti nell'utilizzo dei sistemi informatici.
La Società, inoltre, deve dotarsi di uno strumento che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda, e gli obblighi degli stessi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

Classificazione e controllo dei beni
La Società deve dotarsi di uno strumento che definisca i ruoli e le responsabilità per l'identificazione e la classificazione degli asset aziendali (ivi inclusi dati e informazioni).

Sicurezza fisica
La Società deve dotarsi di uno strumento che disponga l'adozione di controlli, al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni al loro interno contenuti, tramite la messa in sicurezza delle aree e delle apparecchiature.

Gestione delle comunicazioni e dell'operatività
La Società deve dotarsi di uno strumento che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informatici tramite *policy* e procedure. In particolare, tale strumento normativo deve assicurare:

- il corretto e sicuro funzionamento degli elaboratori di informazioni;
- la protezione da software pericolosi;
- il backup di informazioni e *software*;
- la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
- gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- una verifica dei *log* che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
- il controllo sui cambiamenti agli elaboratori e ai sistemi;
- la gestione di dispositivi rimovibili.

Gestione degli incidenti e dei problemi di sicurezza informatica
La Società deve dotarsi di uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica.

In particolare, tale strumento deve prevedere:

- appropriati canali gestionali per la comunicazione degli incidenti ed eventuali problemi;

- l'analisi periodica dei dati di sistema;

- la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;

- l'analisi di *report* e *trend* sugli incidenti e sui problemi e l'individuazione di azioni preventive;

- appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi riscontrata o potenziale;

- l'utilizzo di banche dati per supportare la risoluzione degli incidenti.

Audit/Monitoraggio
La Società deve dotarsi di uno strumento che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica, periodica, dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.

Crittografia
La Società deve dotarsi di uno strumento normativo che preveda l'implementazione e lo sviluppo sull'uso dei controlli crittografici, per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche.

Risorse umane e sicurezza
La Società deve dotarsi di uno strumento che preveda:

- specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, se necessario, per i terzi;

- l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) ai dipendenti e ai terzi al momento della conclusione del rapporto di lavoro e/o del contratto;

- la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

5. Flussi informativi nei confronti dell'OdV

Le Direzioni/Funzioni Aziendali coinvolte garantiscono, coordinando le strutture di propria competenza, la documentabilità del singolo processo monitorato, comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento critico cui sono legati i rischio-reato.

Lo strumento di comunicazione è rappresentato prevalentemente dalla e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it , con la specificazione nell'oggetto del reference del flusso informativo cui si riferisce la comunicazione medesima.

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "C"

DELITTI DI CRIMINALITÀ ORGANIZZATA

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 – 20123 Milano P. IVA – C. F. 12082290961

INDICE

1. Rinvio al catalogo dei reati presupposto

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei delitti di criminalità organizzata di cui agli articoli di cui all'art. 24 *ter* del D. Lgs. 231/2001 che devono essere contemplati anche tenendo conto della fattispecie del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

2. Identificazione delle aree e delle attività sensibili

Di seguito, si evidenziano, in macroaree, le Funzioni/Direzioni aziendali coinvolte nelle fattispecie di attività sensibili:

- Amministratore Unico
- Amministratore designato
- Responsabile Amministrativo
- Impiegato
- Tirocinante

Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati di criminalità organizzata, raggruppate per macro - categorie:

- **Gestione sponsorizzazione ed altri progetti**
- **Gestione convegni e congressi**
- **Selezione del personale**
- **Gestione dei finanziamenti**
- **Acquisto di beni e servizi**
- **Ciclo passivo**
    - Selezione dei consulenti
    - Selezione dei consulenti e intermediari per incarichi professionali riguardanti la gestione risorse umane
- **Gestione dei flussi e delle transazioni finanziarie**
- **Selezione e gestione agenti, grossisti e partner commerciali**
- **Partecipazione a partnership (Joint Ventures, Consorzi, ATI) – Selezione dei partner d'affari**

3. Procedure e programmi applicabili

In relazione alle attività sensibili deve esser fatto divieto di intrattenere relazioni, dirette o indirette, con soggetti di cui sia conosciuta, o di cui si abbia il fondato sospetto, l'appartenenza ad organizzazioni criminali o che comunque operino al di fuori della legalità.

4. Principi generali di comportamento e procedure di prevenzione

Il Modello, in relazione alle attività ritenute sensibili di cui sopra, ai sensi dell'art. 24 *ter* del Decreto, prevede i principi di controllo specifici di seguito indicati:

- è fatto espressamente divieto di intrattenere relazioni, dirette o indirette, con persone delle quali sia conosciuta, o solamente sospettata, l'appartenenza ad organizzazioni criminali o che comunque operino al di fuori della legalità;

- nel caso di richieste, da parte dell'Autorità Giudiziaria, ovvero di controversie legali, indagini, inquisitorie e reclami, è fatto obbligo di cooperare pienamente con le autorità inquirenti in merito ad ogni richiesta e di fornire informazioni veritiere;

- il processo di identificazione del fornitore e la conseguente gestione del rapporto deve prevedere almeno che:

  - al momento dell'attivazione di una qualsiasi relazione di business, il personale della Società deve immediatamente provvedere alla identificazione della controparte;

  - la predisposizione dei contratti con la controparte si basi su standard contrattuali predefiniti;

  - siano previste le principali attività per le singole funzioni coinvolte nel processo di validazione e controllo dei ricevimenti e dei dati contabili che alimentano il processo;

Si precisa che la Società esternalizza, mediante la formalizzazione di un incarico, la gestione del contenzioso giudiziale a legali esterni, che in qualità di destinatari dei presenti principi di comportamento, sono tenuti ad adottare regole di condotta conformi a quanto prescritto.

Eventuali inadempimenti procedurali, laddove possano comportare la commissione di reati rilevanti, saranno sanzionati mediante l'applicazione di provvedimenti disciplinari.

5. Flussi informativi nei confronti dell'OdV

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento

critico cui sono legati i rischio-reato.

Lo strumento di comunicazione è rappresentato prevalentemente dalla e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it, con la specificazione nell'oggetto del reference del flusso informativo cui si riferisce la comunicazione medesima.

SCARANOFUSCA INVESTMENT S.R.L.
Via Dogana, 3 – Milano (20123 – MI)
C.F. / P.I. 12082290961

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "D"

REATI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO E DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 – 20123 Milano P. IVA – C. F. 12082290961

INDICE

1. Rinvio al catalogo dei reati presupposto

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati contro la fede pubblica nonché dei reati contro l'industria ed il commercio, di cui agli artt. 25 *bis* e 25 *bis.1* del D. Lgs. 231/2001, i quali devono essere contemplati anche tenendo conto della fattispecie del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

2. Funzioni coinvolte

Di seguito, si evidenziano, in macroaree, le Funzioni/Direzioni aziendali coinvolte nelle fattispecie di attività sensibili:

- Amministratore Unico
- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

Di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati di contro la fede pubblica nonché ai delitti contro l'industria ed il commercio:

- **Gestione dei flussi e delle transazioni finanziarie**

- **Gestione delle attività commerciali**

- **Partecipazione a partnership (Joint Venture e ATI) - Selezione dei partner d'affari.**

3. Principi generali di comportamento e procedure di prevenzione.

Il Modello, in relazione alle attività ritenute sensibili sopra richiamate prevede i principi di controllo specifici di seguito indicati:

- devono essere stabiliti espressi limiti alla disponibilità di denaro contante e valori bollati (**che dovranno essere sempre entro i limiti di legge**);

- devono essere sempre predisposti verbali/*report* da inviare al superiore gerarchico (e da questi validati) in relazione all'utilizzo di eventuale denaro contante e dei valori bollati, in modo da garantire la tracciabilità delle operazioni.

Tutto il personale coinvolto nei processi di gestione delle transazioni finanziarie è tenuto a comportarsi conformemente alle prescrizioni legislative vigenti ed ai principi richiamati nel Codice etico, astenendosi dall'attuare comportamenti che possano integrare i reati esaminati.

Ai fini della conforme attuazione dei sopra elencati principi di controllo (con riferimento alla concreta identificazione dei ruoli, delle responsabilità e delle modalità di svolgimento), si richiede l'osservanza delle procedure aziendali applicabili che costituiscono parte integrante del Modello. Eventuali inadempimenti procedurali, laddove possano comportare la commissione di reati rilevanti saranno sanzionati mediante l'applicazione di provvedimenti disciplinari.

Il Modello, in relazione alle attività sopra qualificate come sensibili, ai sensi dell'art. 25 *bis* e 25 *bis.1* del Decreto, prevede i principi di controllo specifici di seguito indicati:

- è fatto obbligo di garantire elevati standard qualitativi nello svolgimento delle attività di competenza, nel rispetto della normativa posta a tutela della concorrenza e del mercato;

- per le operazioni riguardanti il trattamento e gestione dei reclami, dei resi e delle note di credito occorre prevedere che:

  - il responsabile interno per l'attuazione dell'operazione garantisca che tutti i reclami ricevuti dalla Società siano sottoposti ad un adeguato controllo tecnico e documentale in conformità con le richieste regolamentari e gli *standard*;

  - tutti i reclami ricevuti siano adeguatamente registrati, classificati e in base alla natura degli stessi e la gravità del presunto difetto, sia effettuata la valutazione del rischio potenziale;

  - le note di credito siano preventivamente autorizzate da soggetti dotati di adeguati poteri;

  - la documentazione riguardante ogni singola attività di processo sia archiviata allo scopo di garantire la completa tracciabilità delle informazioni;

- ove, per la gestione delle succitate attività, vengano utilizzate delle terze parti, garantire che siano qualificate e sottoposte ad audit periodici, nonché che i rapporti con le stesse siano disciplinati tramite specifici contratti contenenti clausole che specifichino:

  - che la terza parte dichiari di rispettare i principi di cui al D. Lgs. 231/2001, nonché di attenersi ai principi di cui al presente Modello ed al Codice Etico;

  - che la terza parte dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzate alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;

- che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c.

4. Principi specifici e procedure di prevenzione

Le operazioni relative alla gestione degli acquisti di prodotti sono regolamentate dalle seguenti procedure di prevenzione e controllo:

- la qualificazione e selezione dei fornitori avviene sulla base di requisiti e criteri predeterminati dalla Società e dalla stessa rivisti con regolare periodicità nonché mediante la stipula di contratti aventi data certa, sottoscritti anche digitalmente, e pervenuti a mezzo pec;

- sono definiti i criteri al fine di prevenire l'utilizzo di prodotti non conformi alla normativa;

5. Flussi informativi nei confronti dell'OdV

Allo scopo di consentire all'Organismo di Vigilanza il monitoraggio e la verifica, in modo tempestivo, circa l'effettiva esecuzione dei controlli previsti dal presente Modello e, in particolare, dalla presente Parte Speciale, nelle procedure sono descritti i flussi informativi che devono essere assicurati al predetto Organismo in conformità a quanto disposto nella Parte Generale del Modello.

L'OdV potrà chiedere alle Direzioni competenti, anche a campione, la documentazione di supporto relativa alle operazioni poste in essere nell'ambito delle "attività sensibili e strumentali".

Le Direzioni/Funzioni aziendali coinvolte garantiscono, coordinando le strutture di propria competenza, la documentabilità del singolo processo monitorato, comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento critico cui sono legati i rischio-reato.

Lo strumento di comunicazione è rappresentato prevalentemente dalla e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it, con la specificazione nell'oggetto del *reference* del flusso informativo cui si riferisce la comunicazione medesima.

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "E"

REATI SOCIETARI

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 – 20123 Milano P.IVA e C. F. 12082290961

INDICE

Introduzione

Per quanto concerne la presente Parte Speciale "*E*", si è ritenuto opportuno trattare in modo congiunto le due categorie di reati di cui agli artt. 25 *ter* e 25 *octies* del D. Lgs. 231/2001 in quanto entrambe riguardano la commissione di illeciti perpetrabili principalmente tramite un uso distorto e/o illecito dei capitali sociali e delle risorse finanziarie.

1. Rinvio al catalogo dei reati presupposto

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati societari e di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, di cui agli artt. 25 *ter* e 25 *octies* del D.Lgs. 231/2001 che devono essere contemplati anche tenendo conto della fattispecie del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

2. Funzioni coinvolte

Di seguito, si evidenziano, in macroaree, le Funzioni/Direzioni aziendali coinvolte nelle fattispecie di attività sensibili:

- Amministratore Unico
- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

Di seguito sono elencate le cosiddette attività sensibili o a rischio:

- **Inserimento variazione o cancellazione dei dati di contabilità nei sistemi informatici di supporto**

- **Valutazioni e stime di poste soggettive di bilancio, rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci e in altri documenti di impresa, ivi compresi quelli tributari**

- **Gestione, documentazione, archiviazione e conservazione delle informazioni relative all'attività d'impresa**

- **Collaborazione e supporto all'organo amministrativo nello svolgimento di operazioni straordinarie**

- **Approvvigionamento di beni e servizi e inserimento anagrafiche fornitori all'interno del sistema**

- **Gestione delle attività amministrativo-contabili e dei pagamenti relativi ad**

approvvigionamento di beni e servizi

- **Attività di dismissione dei cespiti aziendali e relativi adempimenti amministrativo-contabili e di incasso**
- **Attività di eventuale sponsorizzazione e gestione di eventi**
- **Predisposizione e redazione della documentazione necessaria alla presentazione delledichiarazioni fiscali e contributive**

Risultano essere sensibili, inoltre, i seguenti processi:

- **Gestione delle risorse finanziarie (incassi, pagamenti e piccola cassa contante)**
- **Costituzione di R.T.I. o joint venture (con controparti nazionali od estere) relativeall'esecuzione di commesse private o pubbliche**
- **Acquisti di beni o servizi/affidamento di incarichi consulenziali**
- **Impieghi ed investimenti produttivi e/o finanziari**
- **Comunicazioni verso le Autorità Pubbliche di Vigilanza**
- **Scelta dei fornitori**

3. Protocolli comportamentali e procedure di prevenzione

Ai fini dell'attuazione delle regole comportamentali e dei divieti elencati nei paragrafi successivi, i Destinatari della presente Parte Speciale, oltre a dover rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale del presente Modello, devono osservare i seguenti protocolli comportamentali posti a presidio dei rischi-reato sopra identificati (artt. 25 *ter,* 25 *octies* nonché 25 *octies 1* del D. Lgs. 231/2001) e riferibili alle attività sensibili come sopra richiamate e meglio individuate nell'attività di *risk assessment*.

4. Protocolli generali di comportamento

Tutti i Destinatari del Modello, nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle attività sensibili indicate *ut supra*, adottano regole di comportamento conformi ai principi generali di seguito esposti, allo scopo di impedire la commissione dei reati societari ritenuti rilevanti per la Società.

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Parte Speciale, devono essere segnalate dai Destinatari, secondo le modalità previste nella Parte Generale del presente Modello.

In particolare, si stabiliscono i seguenti **principi generali** di comportamento:

- è fatto obbligo di tenere comportamenti trasparenti e corretti, assicurando il rispetto delle norme di legge e regolamentari e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio, alla trasmissione periodica delle informazioni di rilievo contabile;

A tal fine **è fatto divieto** di:

- predisporre o comunicare dati alterati, lacunosi o falsi riguardo alla situazione economica, patrimoniale o finanziaria dell'Ente;
- omettere di comunicare dati o informazioni richieste dalla normativa vigente;
- illustrare i dati e le informazioni utilizzati in modo tale da fornire una rappresentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria dell'Ente e sull'evoluzione della sua attività;
- porre in essere comportamenti che impediscano, mediante l'occultamento di documenti, ovvero con l'uso di altri mezzi fraudolenti, o che, in altro modo, creino ostacoli, lo svolgimento dell'attività di controllo;
- determinare o influenzare l'assunzione delle delibere ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà;

La Società fa espresso obbligo di osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, anche nell'ambito dell'effettuazione di operazioni straordinarie, agendo sempre nel pieno rispetto delle procedure aziendali, al fine di non ledere le garanzie per i creditori o i terzi in generale.

Pertanto, **è fatto divieto** di:

- ripartire utili e/o acconti sugli utili non effettivamente conseguiti, ovvero destinati per legge a riserva, nonché ripartire riserve che per legge non possono essere ripartite;
- acquistare o sottoscrivere quote della società ovvero di eventuali controllanti fuori dai casi previsti dalla legge con lesione dell'integrità del patrimonio sociale;
- effettuare riduzioni di capitale sociale, fusioni e/o scissioni, in violazione delle disposizioni di legge a tutela dei soci o creditori;
- ripartire i beni sociali in danno dei creditori;
- alterare in modo fittizio, con qualsivoglia operazione societaria, il capitale sociale.

Allo scopo di prevenire la commissione di uno degli illeciti indicati all'interno della presente Parte Speciale, deve essere sempre assicurato:

- il regolare funzionamento dell'Ente, garantendo ed agevolando ogni forma di controllo previsto dalla legge, sia di carattere interno, sia di carattere esterno, sulla gestione aziendale;
- la tempestività, la correttezza e la completezza di tutte le comunicazioni previste per legge o regolamento;
- la regolare formazione, tenuta e conservazione di tutta la rilevante documentazione dell'Ente, contabile e fiscale: a tal fine è fatto espresso divieto di tenere comportamenti che, mediante il mancato tempestivo aggiornamento della documentazione, la mancata corretta conservazione o l'occultamento dei documenti impediscano, alle autorità ed agli organi pubblici di vigilanza di effettuare le dovute attività di controllo.

5. Principi specifici di comportamento e procedure comportamentali di prevenzione.

Per tutte le operazioni relative alle attività sensibili individuate nel precedente paragrafo 2, deve essere individuato un Responsabile Interno del procedimento per l'attuazione delle operazioni di propria competenza.

Salvo diversa indicazione, il Responsabile Interno del procedimento si identifica con il Responsabile della Direzione competente per la gestione dell'operazione considerata.

Il Responsabile Interno del procedimento è il diretto responsabile dell'operazione a rischio e deve garantire il rispetto delle regole di condotta, delle politiche, dei principi di comportamento e delle procedure aziendali: lo stesso, in particolare, può chiedere informazioni e chiarimenti a tutte le Direzioni aziendali e a tutti coloro che si occupano ovvero si sono occupati di alcuni aspetti dell'operazione a rischio.

Tutte le operazioni relative alle aree di attività sensibili individuate sono regolamentate dai seguenti protocolli comportamentali specifici di prevenzione e controllo:

- la formazione degli atti e delle decisioni necessarie per lo svolgimento delle operazioni deve essere sempre ricostruibile e deve essere sempre garantito il rispetto dei relativi livelli autorizzativi;
- l'assegnazione dei profili utente all'interno di sistemi informatici deve essere coerente con i ruoli e le responsabilità assegnate;
- i documenti inerenti alle attività poste in essere devono essere sempre archiviati e conservati con modalità tali da non permetterne la modificazione successiva, se non dandone specifica evidenza e consentendone l'accesso soltanto ai soggetti competenti, secondo le normative interne, e agli organi di controllo; l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate e all'Organismo di Vigilanza;
- l'Amministratore Unico comunica all'Organismo di Vigilanza le cariche assunte o le partecipazioni di cui è titolare, direttamente o indirettamente, anche di società esterne, le quali, per la natura o la tipologia, possono lasciar ragionevolmente prevedere l'insorgere di conflitti di interesse;

- nell'impiego delle proprie risorse finanziarie l'Ente si avvale solo di intermediari finanziari e bancari sottoposti ad una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea.

Relativamente all'**attività di inserimento, variazione o cancellazione dei dati di contabilità nei sistemi informatici di supporto** l'Ente prevede che:

- il sistema informatico di supporto deve garantire la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei singoli soggetti che inseriscono i dati nel sistema;
- ai sistemi informatici devono poter accedere unicamente i soggetti autorizzati secondo la normativa interna e in possesso delle necessarie *password*;
- ciascuna autorizzazione deve essere coerente con le specifiche mansioni del titolare cui è concessa e l'accesso deve essere strettamente necessario allo svolgimento delle attività operative dell'Amministratore Unico.

Con riferimento all'**attività relativa alle valutazioni e stime di poste soggettive di bilancio, alla rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci e in altri documenti di impresa**, l'Ente prevede che:

- deve essere adottata, e costantemente aggiornata, una specifica procedura che contempli i criteri contabili da adottare per la definizione delle poste del bilancio civilistico e le modalità operative per la loro contabilizzazione. Tali principi devono essere costantemente e tempestivamente aggiornati nel caso di mutamento del quadro normativo, ovvero della compagine e/o dimensioni sociali.

Relativamente all'attività di gestione, documentazione, archiviazione e conservazione delle informazioni relative all'attività di impresa, la Società prevede:

- che la bozza di bilancio sia sempre messa a disposizione degli amministratori con ragionevole anticipo rispetto alla data della riunione prevista per la sua approvazione;
- che siano presenti piani aziendali di *business continuity* e di *disaster recovery* volti a garantire la conservazione dei dati e delle informazioni relative all'attività di impresa svolta ed al ripristino delle normali funzioni dei sistemi informatici di supporto a seguito di disastri e catastrofi che ne possano compromettere la funzionalità.

Al fine di prendere in considerazione l'opportunità di instaurare rapporti giuridici, di fornitura, collaborazione e comunque rapporti commerciali in genere con altri enti o imprese, l'Ente valuta negativamente:

- imprese che siano da ritenere, anche solo sulla base di elementi di fatto, costituite soltanto allo scopo di occultare o favorire soggetti appartenenti a gruppi criminali o, comunque, di eludere divieti nello svolgimento di attività imprenditoriali;

- imprese od enti che risultino privi di rapporti con aziende di credito;
- l'intervento, nelle trattative commerciali, di persone o enti privi di legittimazione ad interloquire nelle trattative medesime;
- la mancata esibizione di documenti comprovanti l'iscrizione ad albi, ordini, elenchi, qualora l'iscrizione sia requisito necessario per lo svolgimento dell'attività.

L'accertamento delle situazioni di cui ai quattro punti precedenti è indice di inesistente o scarsa affidabilità professionale della controparte, e può comportare la scelta di interrompere le trattative in essere o i rapporti contrattuali già instaurati con fornitori, consulenti, collaboratori o partner accreditati presso la Società.

Tutti i pagamenti o le transazioni finanziarie devono essere effettuati esclusivamente tramite intermediari autorizzati, in modo che ne sia garantita sempre la tracciabilità sulla base di idonea documentazione.

Non sono ammessi pagamenti in contanti, al di sopra dei limiti consentiti dalla legislazione vigente, ovvero mediante assegni liberi.

I Destinatari della presente Parte Speciale del Modello devono astenersi dal partecipare ad attività che siano fonte potenziale di conflitto di interesse e, nel caso in cui ciò avvenga, ne devono dare immediata comunicazione al superiore gerarchico e all'OdV. Sarà cura del Responsabile Interno verificare, periodicamente, che i dipendenti, ed in special modo i soggetti posti a livello apicale, non versino in situazioni di conflitto di interesse con la Società.

Si può derogare ai protocolli comportamentali, specificati *ut supra*, esclusivamente nei casi di necessità e urgenza. In ogni caso, è compito del soggetto che effettua la deroga alla procedura di informare tempestivamente la Funzione/Direzione competente la quale ne darà tempestivamente notizia all'OdV.

6. Flussi informativi verso l'OdV

Al fine di fornire all'Organismo di Vigilanza gli strumenti per esercitare le attività di monitoraggio e di verifica puntuale della efficace esecuzione dei controlli previsti dal presente Modello e, in particolare, dalla presente Parte Speciale, nelle procedure sono descritti i flussi informativi che devono essere assicurati al predetto Organismo, in conformità a quanto disposto nella Parte Generale del Modello medesimo.

L'OdV, in particolare, dovrà essere informato relativamente all'approvazione dei bilanci.

Il Responsabile Interno informa tempestivamente l'OdV di fatti o circostanze significative riscontrate nell'esercizio delle operazioni a rischio della propria Funzione/Direzione, nonché di qualunque ipotesi di reato, criticità sorta nell'ambito delle operazioni societarie; il medesimo garantisce il flusso informativo periodico nei confronti dell'OdV, stilando periodicamente (almeno annualmente) *reports* informativi.

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento cui sono legati i rischio-reato ed i controlli attesi.

Lo strumento di comunicazione è rappresentato prevalentemente dall'e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it con la specificazione nell'oggetto del *reference* del flusso informativo cui si riferisce la comunicazione medesima.

SCARANOFUSCA INVESTMENT S.R.L.
Via Dogana, 3 – Milano (20123 – MI)
C.F. / P.I. 12082290961

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "F"

OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 – 20123 Milano P. IVA – C. F. 12082290961

INDICE

Introduzione

La Legge delega del 3 agosto 2007, n. 123, ha introdotto, nell'articolato del Decreto Legislativo 231/2001, l'art. 25 *septies*, che integra la lista dei reati presupposto con **i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro**.

Le norme antinfortunistiche, dirette alla tutela della salute, della sicurezza e dell'igiene nei luoghi di lavoro richiamate dagli articoli del Codice Penale trovano regolamentazione all'interno del D. Lgs. n. 81/08.

Segnatamente, il D. Lgs. n. 81/08 individua nel **Documento di Valutazione Rischi (DVR)** il perno attorno a cui ruota il sistema di sicurezza dell'impresa.

Il DVR è il documento in cui deve essere formalizzata l'attività di "rilevazione e valutazione di tutti rischi per la salute e la sicurezza dei lavoratori" (ivi compresi quelli riguardanti gruppi di lavoratori particolari), che il datore di lavoro, unitamente agli altri ulteriori soggetti identificati dalla normativa in parola, deve effettuare.

Il processo di valutazione rischi richiesto dal D. Lgs. 81/08 porta all'individuazione e valutazione dei rischi esistenti in capo ai lavoratori nello svolgimento delle rispettive mansioni per ciascuna area aziendale, nonché di ogni ulteriore rischio cui possono incorrere i lavoratori nello svolgimento delle attività aziendali.

Detto documento impone l'ulteriore obbligo di individuare, ed attuare, specifiche misure preventive di tutela volte all'eliminazione, ovvero alla riduzione (entro determinati limiti, ritenendo determinati rischi accettabili e tollerabili in quanto connaturati alla fisiologica esecuzione dell'attività lavorativa) del rischio lavorativo dei dipendenti e/o collaboratori, nonché la predisposizione di idonei **Dispositivi di Protezione Individuale (DPI)**.

1. Rinvio al catalogo dei reati

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti, di cui alla presente Parte Speciale, si rinvia alla lettura estesa dei reati di cui all'art. 25 *septies* del Decreto i quali devono essere contemplati anche nella forma del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

1.1 Breve descrizione delle fattispecie di reato

Le condotte punite dai reati in esame consistono nel cagionare, colposamente, l'evento mortale ovvero lesioni personali gravi o gravissime in capo ai lavoratori (ovvero collaboratori esterni della Società).

Ai fini della commissione di questi reati, rileva una qualsiasi condotta, sia commissiva, sia omissiva (consistente nel non aver impedito il verificarsi dell'incidente che si aveva l'obbligo di impedire, in quanto il soggetto gerarchicamente superiore assume, in relazione a tali fattispecie, una posizione di garanzia).

I reati di cui agli articoli 589 e 590 c.p. sono **reati colposi**, ciò significa che l'evento (morte / lesioni) non è voluto dal soggetto agente ma si è verificato per una **negligente** inosservanza di leggi, ordini e discipline, che mirano a prevenire eventi dannosi o pericolosi da parte di chi aveva l'obbligo di osservarle.

Il concorso di colpa del dipendente non ha alcun effetto esimente (salvo l'ipotesi in cui la condotta del lavoratore si configuri come abnorme, inopinabile ed esorbitante rispetto alle direttive ricevute e al procedimento lavorativo, nonché atipica, eccezionale ed imprevedibile).

2. Il modello con riferimento ai reati presupposto ex art. 25 septies del Decreto

L'art. 5 del D. Lgs. 231/2001, come noto, richiede per la configurabilità della responsabilità in capo all'Ente, anche in caso di commissione dei reati presupposto di cui all'art. 25 *septies* del Decreto, che il reato sia stato commesso nell' "*interesse e/o a vantaggio*" dell'ente stesso.

In considerazione della natura colposa dei reati in esame si ritiene che **l'interesse e/o vantaggio per l'ente si possa ravvisare nel risparmio di costi e/o tempi ottenuti a seguito della mancata osservanza delle norme poste a presidio della tutela della salute e sicurezza dei dipendenti**.

Anche la causa di esclusione della responsabilità per l'ente di cui all'art. 6 del D.Lgs. 231/01, deve essere valutata in relazione alla struttura colposa del reato. Essa, infatti, da una interpretazione letterale della norma, sembrerebbe coerente con le sole fattispecie dolose: ciò in quanto l'assenza della colpevolezza dell'ente, che presuppone l'invocabilità dell'esimente, deriva dalla dimostrazione che il reato è stato realizzato aggirando, fraudolentemente, il sistema di controlli stabilito per prevenire la tipologia di reato considerata in concreto.

Ne deriva che, in relazione ai reati di natura colposa, rispetto ai quali la volontarietà è limitata alla sola condotta e non anche all'evento, per l'applicabilità dell'esimente non sarà possibile dimostrare che l'agente abbia cagionato la verificazione dell'evento aggirando fraudolentemente il Modello.

Sarà, al contrario, necessario dimostrare che la condotta, in concreto, è stata posta in essere dall'agente **in modo volontario e consapevole** (ponendo in essere un comportamento imprudente e/o negligente), disattendendo le regole e le procedure interne che l'ente si è dato per garantire il pieno rispetto delle norme in materia di sicurezza e salute dei dipendenti, e nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito organismo a ciò preposto.

3. Identificazione delle aree e delle attività sensibili

Di seguito, si evidenziano, in macroaree, le Funzioni/Direzioni aziendali coinvolte nelle fattispecie di attività sensibili:

- Amministratore Unico
- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

È opportuno precisare che tutte le attività aziendali debbono considerarsi, in astratto, attività nello svolgimento delle quali un dipendente e/o un collaboratore, anche esterno, potrebbe subire un infortunio e pertanto sono state tutte prese in considerazione dal DVR adottato dalla Società.

Il documento, in modo dettagliato, prende in considerazione l'intero ciclo produttivo aziendale e tutte le aree di rischio in concreto riscontrabili all'interno dei locali della Società.

In osservanza dell'art. 29, co. 4, D. Lgs. 81/2008 il documento è custodito presso l'unità produttiva alla quale si riferisce la valutazione dei rischi.

Nel DVR sono indicate, in modo specifico e dettagliato, le misure di sicurezza che la Società ha inteso attuare allo scopo di ridurre i rischi relativi ai luoghi di lavoro; tutte le procedure devono intendersi ivi integralmente richiamate.

La Società si impegna a tenere sempre aggiornato il proprio DVR, onde mantenere sempre efficaci e tecnicamente corrette le procedure ivi contenute.

Fermo restando quanto sopra, ai fini dell'implementazione del Modello, con riferimento ai reati presupposto di cui all'art. 25 *septies*, la Società ha considerato di fondamentale importanza:

- verificare che il proprio sistema organizzativo garantisca, su base continuativa ed in maniera formalizzata, lo svolgimento delle attività lavorative nel pieno rispetto e nella corretta applicazione delle norme antinfortunistiche e degli standard di sicurezza posti a presidio della salute e dell'integrità fisica dei dipendenti;

- ove necessario adeguare detto sistema organizzativo alla normativa vigente.

La Società, ai sensi dell'art. 6 del Decreto ha, pertanto, individuato all'interno delle aree di rischio/sensibili, come attività a potenziale rischio di violazione delle norme antinfortunistiche, le seguenti aree/attività:

- **attività di valutazione dei rischi, individuazione delle misure di protezione e prevenzione ed aggiornamento delle stesse (Datore di lavoro, Delegato alla sicurezza, RSPP);**

- **attività di organizzazione interna in materia di:**

  - antinfortunistica/sicurezza;

  - attività di verifica periodica del sistema organizzativo in essere, dell'applicazione ed efficacia delle procedure, dell'aggiornamento dei ruoli e responsabilità;

  - attività di verifica e ispezione programmata dei luoghi e delle attività, ivi comprese quelle sui mezzi ed attrezzature di lavoro (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico competente);

- **attività di formazione ed informazione in materia di sicurezza** (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico competente)**;**

- **attività di rilevazione degli incidenti ed infortuni sul lavoro** (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico competente);

- **manutenzione dei luoghi di lavoro e delle apparecchiature in maniera da garantirne l'idoneità, la sicurezza e la conformità alle prescrizioni di legge** (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico competente);

- **attività dirette a garantire adeguata ed idonea segnaletica all'interno di tutti i luoghi di lavoro ed adeguati mezzi di protezione individuale ai dipendenti** (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico competente);

- **attività di prevenzione incendi e gestione delle emergenze e primo soccorso** (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico competente);

- attività di selezione degli appalti e dei prestatori d'opera (Datore di lavoro, Delegato alla sicurezza, RSPP, Medico Competente).

4. Protocolli generali di comportamento

Il presente Modello non si sostituisce agli obblighi e alle responsabilità di legge disciplinate, in capo ai soggetti individuati, dal D. Lgs. 81/08 e dalla normativa ulteriormente applicabile in materia di sicurezza, salute ed igiene del lavoro.
Costituisce, al contrario, un presidio ulteriore di controllo e verifica dell'esistenza, efficacia ed adeguatezza della struttura ed organizzazione posta in essere in ossequio alla normativa settoriale vigente.

Deve, pertanto, intendersi presupposto e parte integrante del presente Modello, tutta la documentazione predisposta dalla Società per l'assolvimento degli obblighi imposti dalla normativa antinfortunistica quale, in via esemplificativa, il DVR.

La figura del RSPP è rappresentata dal Sig. Salvatore Scarano.

È presente, altresì, il Rappresentante per la sicurezza dei lavoratori individuato nella persona della Sig.ra Roberta Mammolenti.

Il Medico Competente risulta essere il Dott. Achille Capria, dotato di specifiche competenze che non versa in situazioni di incompatibilità con i compiti affidati.

Le deroghe, le violazioni e/o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Parte Speciale devono essere oggetto di segnalazione espressa da parte di tutti i dipendenti (anche esterni) e di tutti gli organi sociali, secondo le modalità previste nella Parte Generale del presente Modello.

È fatto **obbligo** ai Destinatari del Modello che si trovino legittimamente presso i locali dell'Ente, di:

- rispettare le disposizioni di legge e, con particolare riferimento ai lavoratori, le previsioni di cui all'art. 20 del D. Lgs. 81/08, la normativa interna, di cui fa parte il presente protocollo, e le istruzioni impartite in materia di sicurezza anche con specifico riferimento alla mansione ricoperta ed all'utilizzo di DPI;

- agire osservando tutte le disposizioni di legge, la normativa interna e le istruzioni impartite in materia di sicurezza;

- astenersi dall'adottare comportamenti imprudenti rispetto alla salvaguardia della propria salute e della propria sicurezza;

- esercitare ogni opportuno controllo ed attività idonea a salvaguardare la salute e la sicurezza dei collaboratori esterni e/o di persone estranee, eventualmente presenti sul luogo di lavoro;

- utilizzare correttamente, secondo le istruzioni impartite e le procedure esistenti, le apparecchiature informatiche, gli utensili, nonché i dispositivi di sicurezza;

- segnalare immediatamente a chi di dovere le anomalie dei dispositivi di cui ai punti precedenti, nonché le altre eventuali condizioni di pericolo di cui si viene a conoscenza;

- adoperarsi direttamente, compatibilmente con le proprie competenze e possibilità, senza mettere a repentaglio la propria vita, a fronte di un pericolo rilevato, sempre che si tratti di casi di urgenza;

- sottoporsi ai controlli sanitari previsti;

- effettuare le attività formative e di aggiornamento previste;

- contribuire all'adempimento di tutti gli obblighi imposti dalle autorità competenti, ovvero comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante le attività lavorative.

Si ricorda che l'art. 20 del D. Lgs. 81/2008, rubricato "obblighi dei lavoratori", testualmente dispone:

1. Ogni lavoratore deve prendersi cura della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.
2. I lavoratori devono in particolare:
a) contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
b) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi i mezzi di trasporto nonché i dispositivi di sicurezza;

È fatto espresso **divieto**, quindi, a tutti i Destinatari del Modello di:

- rimuovere e/o modificare, senza previa autorizzazione espressa e formale, i dispositivi di sicurezza o di segnalazione o di controllo;

- effettuare, in mancanza di specifica autorizzazione, operazioni ovvero manovre che non siano di propria competenza, o ancora che possano compromettere la sicurezza propria e/o di altri lavoratori.

5. Principi specifici di comportamento e procedure di prevenzione

Quanto alle misure di prevenzione per le attività sensibili soggette al rischio di commissione dei reati *ex* art. 25 *septies* del Decreto, ovvero di quei comportamenti che potrebbero integrare la responsabilità della Società in relazione a infortuni sul lavoro, nell'attuazione del proprio sistema organizzativo, con specifico riferimento alla sicurezza aziendale e nello svolgimento delle attività dallo stesso programmate, l'Ente ed i Destinatari del presente Modello, ciascuno per le proprie competenze, dovranno attuare e rispettare i seguenti principi specifici di comportamento/protocolli di prevenzione:

Valutazione dei rischi e individuazione delle misure di protezione e prevenzione, ed aggiornamento delle stesse:

- deve essere adeguatamente effettuata, ed aggiornata su base continuativa, la valutazione di tutti i rischi per la sicurezza e la salute dei lavoratori nei luoghi di lavoro, in applicazione di quanto previsto dal D. Lgs. 81/08 e da tutta la normativa antinfortunistica applicabile, tenendo altresì adeguatamente conto di ogni mutamento intervenuto nei processi produttivi, nell'organizzazione del lavoro e/o dei luoghi di lavoro;

- tutti i dati e le informazioni che servono alla valutazione dei rischi e, conseguentemente, all'individuazione delle misure di tutela (es. documentazione tecnica etc.) devono essere chiari, completi e rappresentare in modo veritiero lo stato dell'arte dei macchinari della Società, dovendo

tutto il complesso degli strumenti aziendali essere dotato di regolare omologazione;

- deve esser data attuazione alle misure di prevenzione e protezione dai rischi come identificati, tenendo costantemente aggiornate le relative procedure;

- devono essere sempre aggiornati eventuali rischi specifici e devono essere attuate le misure di protezione relative;

- il Medico Competente deve attuare un adeguato programma di sorveglianza sanitaria, ai sensi dell'art. 41 del D. Lgs. 81/08;

- il Medico Competente comunica al Datore di lavoro il Protocollo Sanitario e l'organizzazione delle visite mediche al personale;

Attività di organizzazione interna in materia di antinfortunistica e sicurezza (deleghe/procure, approvazione dei budget di spesa, procedure interne) attività di verifica periodica del sistema organizzativo interno, dell'applicazione ed efficacia delle procedure previste, dell'aggiornamento dei ruoli e responsabilità, attività di verifica ed ispezione programmata dei luoghi e delle attività:

- le eventuali deleghe in materia di sicurezza del lavoro e sulla tutela dell'igiene e salute sul lavoro sono redatte per iscritto determinando in modo chiaro, specifico ed univoco le funzioni assegnate, assicurando la coerenza del sistema delle deleghe, dei poteri di firma e di spesa con le responsabilità assegnate;

- sono correttamente nominati tutti i soggetti previsti dalla normativa in materia di igiene, salute e sicurezza dei luoghi di lavoro e devono essere conferite adeguate direttive e poteri necessari allo svolgimento dei ruoli assegnati;

- sono resi noti, a tutti i livelli dell'organizzazione, le funzioni, i compiti e le responsabilità del Responsabile del Servizio di Prevenzione e Protezione (RSPP) e degli addetti alla gestione delle emergenze, nonché i compiti e le responsabilità del Medico competente, anche attraverso la predisposizione da parte del RSPP di un apposito Organigramma della Sicurezza;

- l'Organigramma della Sicurezza è comunicato a tutto il personale e/o affisso in bacheca o altro luogo cui possano accedere i lavoratori;

- sono previste apposite modalità di aggiornamento costante nel tempo delle procedure operative, anche al fine di valutare l'adeguatezza delle medesime.

Attività di formazione ed informazione in materia di sicurezza:

- è garantita adeguata conoscenza della normativa applicabile in materia infortunistica ai soggetti responsabili della sicurezza, ivi compresi dirigenti e

soggetti preposti alla sicurezza, al Responsabile interno, nonché agli addetti al sistema prevenzione e protezione ed agli addetti di pronto soccorso ed emergenza;

- è adeguatamente programmata ed effettuata la formazione ed informazione dei dipendenti – anche a tempo determinato – e dei collaboratori sulle disposizioni in materia di antinfortunistica in generale, nonché sui rischi specifici cui essi sono sottoposti in relazione alle mansioni assegnate, e sulle misure di prevenzione e comportamenti da adottare. In particolare vengono svolte, con cadenza periodica (da stabilirsi a cura degli organi apicali in coordinamento con il RSPP) prove di evacuazione dirette dal RSPP con relativo report che viene posto alla diretta attenzione dell'Amministratore Unico e per conoscenza, dell'OdV;

- il personale è costantemente formato ed informato in merito alle misure di prevenzione e protezione adottati e deve essere pienamente consapevole degli obblighi ai quali è tenuto per la protezione della propria incolumità e della propria salute, nonché dell'incolumità e salute dei colleghi e dei terzi;

- la partecipazione ai corsi è registrata in appositi moduli compilati dai partecipanti, ed archiviata, in forma cartacea o informatica, in appositi "libretti di formazione del lavoratore";

- sono predisposti appositi sistemi di verifica dell'apprendimento a conclusione delle sessioni formative, che dovranno essere registrati ed archiviati "nel libretto formazione del lavoratore";

Attività di rilevazione degli incidenti ed infortuni sul lavoro e di eliminazione delle cause degli stessi, ovvero riduzione ad un livello di rischio accettabile:

- è effettuata adeguata registrazione, in apposito "registro infortuni", del monitoraggio e dell'analisi degli infortuni sul lavoro, nonché delle malattie professionali e delle relative cause, anche al fine di ridurne l'incidenza;

- ogni sinistro occorso, anche di lieve entità, deve essere portato all'attenzione del RSPP, agli organi apicali, oltre che all'OdV per conoscenza;

- possono essere affidate ad esperti esterni periodici *audit* tecnici dei luoghi e delle attività di lavoro e dell'organizzazione della sicurezza aziendale.

Attività di predisposizione e manutenzione dei luoghi di lavoro, degli impianti e delle attrezzature aziendali in maniera idonea a garantirne l'idoneità, la sicurezza e la conformità alle prescrizioni di legge:

- le attività di acquisto di apparecchiature ed impianti informatici sono condotte valutando preventivamente i requisiti di sicurezza inerenti le stesse, eventualmente acquisendo il parere del RSPP;

- le apparecchiature ed impianti informatici dovranno essere conformi a quanto previsto dalla normativa vigente (es. marcatura comunitaria, possesso di dichiarazione di conformità rilasciata dall'installatore); se del caso, in ragione dei disposti legislativi applicabili, la loro messa in esercizio sarà subordinata a procedure di esame iniziale ovvero di omologazione;

- tutte le attrezzature, le apparecchiature e gli impianti, o acquisto/noleggio che possono avere impatti significativi in materia di salute e sicurezza sono assoggettati a protocolli di manutenzione programmata con tempistiche e modalità anche definite con l'ausilio dell'RSPP. Gli eventuali interventi specialistici saranno condotti da soggetti in possesso dei requisiti di legge che dovranno produrre le necessarie documentazioni;

- le attività di manutenzione su dispositivi di sicurezza devono essere oggetto di registrazione in apposito manuale di ogni singolo macchinario e/o impianto;

- è data tempestivamente notizia al RSPP dell'introduzione di eventuali variazioni sostanziali dei macchinari, delle apparecchiature all'interno dei luoghi di lavoro.

Attività dirette a garantire adeguata segnaletica nei luoghi di lavoro:

- è predisposta e mantenuta aggiornata una adeguata segnaletica all'interno dei luoghi di lavoro;

- la consegna dei dispositivi di protezione individuale ai dipendenti è comprovata dall'apposizione di una firma per ricevuta da parte dei dipendenti in apposito registro da conservarsi a cura del RSPP.

Attività di prevenzione incendi e gestione delle emergenze e primo soccorso:

- devono essere adeguatamente organizzate le risorse poste a presidio del soccorso e dell'emergenza, ed adeguatamente predisposte e formalizzate le procedure e i manuali di gestione delle emergenze, anche effettuando prove periodiche;
- tra il personale sono individuati gli addetti agli interventi di emergenza; essi devono essere individuati in numero sufficiente e preventivamente formati secondo i requisiti di legge;

- sono disponibili e mantenuti in efficienza idonei sistemi per la lotta agli incendi; tali sistemi antincendio sono scelti per tipologia e numero in ragione della specifica valutazione del rischio di incendio ovvero delle indicazioni fornite dall'autorità competente; sono altresì presenti e mantenuti in efficienza idonei presidi sanitari;

- la gestione delle emergenze è attuata attraverso specifici piani, adeguati ed effettivamente attuati, che prevedono:

- l'identificazione preventiva, ove oggettivamente possibile, delle situazioni che possono causare una potenziale emergenza;

- le modalità operative concrete da attuare al fine di prevenire l'insorgere di situazioni di emergenza ovvero mitigare i potenziali effetti negativi derivanti dalle stesse;

- la verifica periodica, pianificata, al fine di valutare l'efficacia dei piani di gestione delle emergenze.

Attività di selezione degli appalti e dei prestatori d'opera in qualità di committente:

- le attività in appalto e le prestazioni d'opera da svolgersi all'interno delle sedi della Società sono disciplinate dall'art. 26 e dal Titolo IV del D. Lgs. 81/08;

- l'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi deve rilasciare la "Dichiarazione di conformità alle regole dell'arte";

- è adeguatamente verificata l'idoneità tecnico professionale, e quella in materia di adempimenti della sicurezza sul lavoro delle imprese o dei lavoratori autonomi, che siano chiamati a svolgere le loro attività presso la Società, effettuando una idonea analisi e valutazione dei rischi derivanti da eventuali interferenze;

- per quanto riguarda i lavori affidati in appalto a ditte esterne, si prevedono misure di coordinamento dettagliate. La responsabilità in tal caso resta in capo al Datore di Lavoro che, attraverso il servizio di prevenzione e protezione, ha la responsabilità di predisporre, divulgare e far attuare le misure di cooperazione e coordinamento, volte alla tutela dei lavoratori in caso di affidamento di lavori all'interno dell'Azienda. Sia il modulo di valutazione rischi, sia il modello relativo agli oneri sulla sicurezza, debitamente compilati, devono essere inseriti, obbligatoriamente, quali allegati, o quantomeno richiamati, del contratto di appalto; segnatamente il RSPP ha cura di portare all'attenzione dell'impresa appaltatrice il DVR della Società il quale sarà allegato al contratto che verrà sottoscritto con l'impresa appaltatrice medesima;

- nel caso in cui la Società, in qualità di committente, apra un cantiere temporaneo o mobile ai sensi del titolo IV del D. Lgs. 81/08, la stessa nomina un direttore dei lavori e provvede a tutti gli adempimenti in materia di sicurezza richiesti dalla legge.

Per il controllo dell'effettiva implementazione delle disposizioni previste dalla normativa vigente in materia antinfortunistica, tutela della sicurezza e della salute nei luoghi di lavoro:

- Il RSPP fornisce una sintesi del DVR vigente (oppure ne garantisce la libera consultazione) ed informa l'OdV circa sostanziali aggiornamenti del medesimo documento aziendale (fornendo copia, per conoscenza, al datore di lavoro);

- il datore di lavoro assicura che siano nominati tutti i soggetti previsti dalla normativa di settore;

- il datore di lavoro assicura, altresì, che tali soggetti dispongano delle competenze e qualità necessarie;

- l'RSPP comunica al datore di lavoro, ovvero al dirigente delegato, ed all'OdV per conoscenza, ogni impedimento all'esercizio delle proprie funzioni affinché siano adottati provvedimenti opportuni;

- ai fini delle attività di controllo summenzionate possono essere condotte attività di *audit*, eventualmente anche a cura dell'OdV, anche con la collaborazione dei soggetti aziendali competenti o di consulenti esterni;

- l'RSPP ed il Medico Competente comunicano al Datore di lavoro, e all'OdV per conoscenza, il programma delle visite ispettive annuali programmate ed i verbali delle visite di controllo, nonché delle ispezioni tecniche (specificando ove programmate ed ove a sorpresa) effettuate, evidenziando eventuali non conformità e comunicandole immediatamente all'Amministratore Unico e per conoscenza all'OdV;

- l'RSPP e il Datore di lavoro comunicano all'OdV:

  - il programma annuale di formazione dei dipendenti;

  - il programma annuale delle attività di manutenzione ordinaria e straordinaria;

- il RSPP ed il Medico Competente comunicano, senza indugio, al Datore di lavoro, e per conoscenza all'OdV, tutti i casi di inefficacia, inadeguatezza e/o difficoltà in attuazione dei principi/protocolli di prevenzione, al fine di ottenere chiarimenti in merito agli obiettivi ed alle modalità di prevenzione previste dal Modello, anche con riferimento a quanto contenuto all'interno del DVR; analoga procedura deve essere svolta nel caso in cui sia il Responsabile Interno a scorgere casi di inefficacia, inadeguatezza e/o difficoltà di attuazione dei principi/protocolli contenuti nel Modello;

- il Datore di lavoro, l'RSPP ed il Medico Competente aggiornano periodicamente (**almeno annualmente**) gli amministratori (e per conoscenza l'OdV) della Società in merito alle tematiche relative alla sicurezza sui luoghi di lavoro, ed in particolare **fornendo copia del verbale relativo alla riunione annuale di sicurezza prevista dalla normativa**;

- in caso di ispezioni amministrative relative agli adempimenti di cui al D.Lgs. 81/08, o comunque inerenti ad aspetti della sicurezza, partecipano i soggetti a ciò espressamente delegati. **L'OdV dovrà essere informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della Funzione aziendale di volta in volta interessata**; in caso di rilievi mossi dall'autorità di controllo, dovrà essere informato anche l'OdV per opportuna conoscenza;

- le attività di monitoraggio e verifica della gestione in materia di sicurezza che possono essere condotte dall'OdV sono effettuate periodicamente e formalizzate e trasmesse agli amministratori, al Datore di Lavoro e al RSPP;

- l'OdV, nell'esercizio delle sue funzioni, può chiedere l'assistenza di soggetti nominati dalla Società, nonché di competenti consulenti esterni.

6.Flussi informativi in favore dell'OdV

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento cui sono legati i rischio-reato ed i controlli attesi. Lo strumento di comunicazione è rappresentato prevalentemente dall'e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it, con la specificazione nell'oggetto del *reference* del flusso informativo cui si riferisce la comunicazione medesima.

L'OdV propone, ove ne emerga la necessità, le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione, anche in caso di evoluzione normativa, ovvero mutamento della composizione e/o dimensione dell'Ente.

SCARANOFUSCA INVESTMENT S.R.L.
Via Dogana, 3 – Milano (20123 – MI)
C.F. / P.I. 12082290961

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "G"

IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 - 20123 Milano P. IVA – C. F. 12082290961

INDICE

Introduzione

Il 9 agosto 2012 è entrato in vigore il D. Lgs. 16 luglio 2012 n. 109 che, dando attuazione alla direttiva 2009/52/CE, ha introdotto norme minime relative a sanzioni e a provvedimenti nei confronti dei datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorno è irregolare.

La norma ha inoltre introdotto nel Decreto il nuovo art. 25 *duodecies,* intitolato "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*", che ha esteso la responsabilità dell'ente anche al delitto previsto dall'art. 22 comma 12 *bis* del D.Lgs. 25 luglio 1998 n. 286.

Nello specifico, tale norma prevede che: << *Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000 euro per ogni lavoratore impiegato. 12-bis. Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà: a) se i lavoratori occupati sono in numero superiore a tre; b) se i lavoratori occupati sono minori in età non lavorativa; c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale.*>>

1. Rinvio al catalogo dei reati

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati di cui all'art. 25 *duodecies* D. Lgs. 231/2001, tenendo conto delle fattispecie del tentativo (art. 56 c.p.) e del concorso di persone nel reato (art. 110 c.p.).

2. Identificazione delle aree e delle attività sensibili

La Società ha dedicato al reato di impiego di personale irregolare una specifica parte speciale al fine di dettare alcune norme generali di comportamento, cui i Destinatari sono tenuti ad uniformarsi, per sottolineare ulteriormente il rispetto della persona, che costituisce uno dei principi cardine del Codice Etico adottato dalla Società.

A tal fine, si precisa che nonostante il c.d. reato di "caporalato" di cui all' 603 bis c.p. ("Intermediazione illecita e sfruttamento del lavoro") non sia incluso nell'ambito dei reati presupposto (con esclusione quindi per tale fattispecie della responsabilità amministrativa dell'ente), la Società, dato il richiamo indiretto a tale reato contenuta nell'art. 22 comma 12 bis del D. Lgs. 25 luglio 1998 n. 286 (reato presupposto di cui al nuovo art. 25 *duodecies* del Decreto), detterà anche in relazione a tale condotta, ad ulteriore tutela della correttezza del proprio operato in tema di assunzioni, alcuni principi specifici di comportamento.

Di seguito, si elencano, raggruppate per macroaree, le Funzioni/Direzioni aziendali responsabili di eseguire e monitorare le attività sensibili:

- Amministratore Unico

- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

Nel corso delle attività di valutazione dei rischi sono stati individuati, come sopra richiamati, gli ambiti aziendali caratterizzati dal rischio di commissione dei reati di cui alla presente Parte Speciale.

In particolare, la mappatura delle attività a rischio, in relazione ai reati di cui all'art. 25 *duodecies* del Decreto ha consentito di individuare alcune attività astrattamente idonee a dar luogo alla responsabilità della Società:

A) In relazione reato di *impiego di cittadini di paesi terzi il cui soggiorno è irregolare* (art. 22 comma 12 bis del Dlgs 286 del 1998) l'area a rischio di commissione del reato presupposto è quella relativa all'assunzione di cittadini stranieri, in primo luogo extracomunitari, mediante qualsivoglia tipologia contrattuale.

Nell'ambito dell'area suddetta, sono state individuate le seguenti attività operative che possono comportare la commissione del suddetto reato:

- **Gestione degli adempimenti propedeutici alla ricerca e selezione del personale**

- **Gestione degli adempimenti relativi alla predisposizione dei contratti di lavoro**

- **Gestione degli adempimenti relativi alla verifica della regolarità dei permessi di soggiorno e alla verifica costante della loro validità, affinché venga chiesto il rinnovo nei termini di legge**.

B) L'area a rischio di commissione dei reati di *procurato ingresso illecito di stranieri* e *favoreggiamento dell'immigrazione clandestina* di cui all'art. 12 c. 3, 3 bis, 3 ter, del D. Lgs. 286/98), nonché di favoreggiamento della permanenza illecita di stranieri nel territorio dello Stato di cui all'art 12 c. 5 D. Lgs. 286/98) può essere individuata in tutte quelle attività connesse al *core business* aziendale che potrebbero facilitare l'occultamento e il trasporto di cittadini stranieri irregolari all'interno e al di fuori dei confini nazionali.
Nell'ambito dell'area suddetta, sono state individuate le seguenti attività operative che possono comportare la commissione del suddetto reato:

- **Gestione dei rapporti con fornitori, appaltatori e subappaltatori**

- **Approvvigionamenti di beni e servizi**

3. Principi generali di comportamento e procedure di prevenzione dei rischi

La Società si impegna al rispetto dei seguenti principi generali e regole di

comportamento, che costituiscono adempimenti richiesti anche a tutti i Destinatari del Modello:

- è fatto assoluto divieto di impiegare lavoratori stranieri privi del permesso di soggiorno, o con un permesso revocato o scaduto, del quale non sia stata presentata rituale domanda di rinnovo, documentata dalla relativa ricevuta;

- la Società si impegna ad identificare i ruoli, i compiti e le responsabilità nel processo di assunzione del personale, predisponendo un idoneo sistema di deleghe e poteri, con idonea pubblicità interna all'azienda, oltre che esterna;

- la Società, nel processo di assunzione di cittadini provenienti da Paesi terzi o extra UE, verifica preliminarmente il rilascio in favore dei medesimi cittadini di valido documento disoggiorno che li abiliti a prestare lavoro in Italia;

- in sede di selezione ed assunzione la Società si impegna a rispettare scrupolosamente le disposizioni del Testo Unico sull'Immigrazione;

- la Società verifica costantemente l'esistenza e la regolarità del permesso di soggiorno esibito in sede di assunzione; la Società si impegna altresì a verificare periodicamente la regolarità del documento di soggiorno, controllando che il lavoratore abbia tempestivamente provveduto alla richiesta di rinnovo prima della sua scadenza, in modo da monitorare la validità dello stesso nel tempo;

- per il reclutamento dei lavoratori è fatto divieto assoluto di procedere all'assunzione di personale tramite intermediari diversi dalle Agenzie per il lavoro autorizzate dal Ministero del Lavoro. Nel caso in cui si faccia ricorso al lavoro interinale mediante agenzie autorizzate, la Società si accerta che tali soggetti si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno, e richiede espressamente all'Agenzia medesima l'impegno a rispettare il Modello;

- in caso di ricorso alle Agenzie autorizzate dal Ministero del lavoro per il reclutamento del personale, la Società verifica il rispetto della normativa vigente in merito alla corresponsione dei trattamenti retributivi e dei contributi previdenziali; ciò attraverso la previsione dell'obbligo a carico di tali Agenzie, pena la risoluzione del contratto, di fornire idonea documentazione comprovante l'adempimento dei relativi obblighi retributivi e previdenziali;

- la Società prevede meccanismi di archiviazione della documentazione acquisita ai fini della verifica del regolare possesso del permesso di soggiorno;

- sono previste, anche contrattualmente, specifiche misure sanzionatorie conseguenti alla scadenza del permesso di soggiorno o al mancato rispetto dei termini previsti per l'invio della domanda di rinnovo;

- la Società si assicura, con apposite clausole contrattuali, che eventuali soggetti terzi con cui collabora (fornitori, consulenti, etc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno.

4. Flussi informativi nei confronti dell'Organismo di Vigilanza

Tutti i Destinatari del Modello hanno l'obbligo, non appena riscontrano un evento anche solo potenzialmente idoneo a configurare uno dei reati presupposto di cui alla presente Parte Speciale, di dare immediato avviso, oltre che a propri superiori gerarchici, anche all'OdV tramite apposita comunicazione.

L'OdV può, in qualsiasi momento, effettuare controlli, anche a sorpresa all'interno dei siti produttivi ed accedere a tutta la documentazione relativa alle attività "sensibili".

In particolare, tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento cui sono legati i rischio-reato ed i controlli attesi.

Lo strumento di comunicazione è rappresentato prevalentemente dall'e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it, con la specificazione nell'oggetto del *reference* del flusso informativo cui si riferisce la comunicazione medesima.

SCARANOFUSCA INVESTMENT S.R.L.
Via Dogana, 3 – Milano (20123 – MI)
C.F. / P.I. 12082290961

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001

PARTE SPECIALE "H"

REATI TRIBUTARI

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data 01/03/2024	Firma SCARANOFUSCA INVESTMENT S.R.L. Via Dogana, 3 - 20123 Milano P. IVA – C. F. 12082290961

INDICE

1. *Rinvio al catalogo dei reati*

Ai fini di una migliore comprensione della normativa in tema di responsabilità amministrativa degli enti di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati di cui all'art. 25 *quinquiesdecies* D.Lgs. 231/2001, tenendo conto delle fattispecie di tentativo (art. 56 c.p.) e di concorso di persone nel reato (art. 110 c.p.).

2. *Identificazione delle aree e delle attività sensibili*

Le fattispecie di reato, a livello apicale, potrebbero essere astrattamente attribuite in capo a:

- Amministratore Unico
- Amministratore designato
- Responsabile amministrativo
- Impiegato
- Tirocinante

Le citate funzioni sono competenti relativamente alle attività di:

- **Inserimento variazione o cancellazione dei dati di contabilità nei sistemi informatici disupporto**
- **Gestione degli adempimenti propedeutici alla presentazione delle dichiarazioni fiscali**
- **Gestione degli adempimenti relativi alla presentazione delle dichiarazioni fiscali**
- **Corretta corresponsione ed assolvimento delle obbligazioni tributarie**
- **Corretta tenuta della documentazione contabile**
- **Corretta gestione del ciclo di fatturazione e dell'eventuale emissione di note di credito**
- **Valutazioni e stime di poste soggettive di bilancio, rilevazione, registrazione e rappresentazione dell'attività della Società nelle scritture contabili, nei bilanci e in altri documenti di impresa, ivi compresi quelli tributari**
- **Approvvigionamento di beni e servizi e inserimento anagrafiche fornitori all'interno del sistema.**

3. *Protocolli comportamentali e procedure di prevenzione*

Ai fini dell'attuazione delle regole comportamentali e dei divieti elencati nei paragrafi successivi, i Destinatari della presente Parte Speciale, oltre a dover rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale del presente Modello, devono osservare i seguenti protocolli comportamentali posti a presidio dei rischi-reato sopra identificati.

4. Protocolli generali di comportamento

Tutti i Destinatari del Modello, nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle attività sensibili indicate *ut supra*, adottano regole di comportamento conformi ai principi generali di seguito esposti, allo scopo di impedire la commissione dei reati tributari ritenuti rilevanti per la Società.

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Parte Speciale, devono essere segnalate da parte di tutti i dipendenti e dagli organi sociali, secondo le modalità previste nella Parte Generale del presente Modello.

In particolare, si stabiliscono i seguenti **principi generali** di comportamento:

- è fatto obbligo di tenere comportamenti trasparenti e corretti, assicurando il rispetto delle norme di legge e regolamentari e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione dei documenti contabili necessari alla predisposizione delle dichiarazioni tributarie.

A tal fine è fatto **divieto** di:

- predisporre o comunicare dati alterati, lacunosi o falsi riguardo alla situazione economica, patrimoniale o finanziaria della Società;

- porre in essere comportamenti che impediscano, mediante l'occultamento di documenti, ovvero con l'uso di altri mezzi fraudolenti, o che, in altro modo, creino ostacoli, al corretto adempimento delle obbligazioni tributarie ed alla formazione delle relative dichiarazioni;

- porre in essere atti simulati o fraudolenti finalizzati alla sottrazione fraudolenta dei beni sociali anche al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

La Società fa espresso obbligo di osservare scrupolosamente tutte le norme poste dalla legge a tutela della veridicità delle dichiarazioni tributarie, agendo sempre nel pieno rispetto dell'intera normativa e delle procedure aziendali, al fine di non ledere le garanzie per il fisco.

Pertanto **è fatto divieto** di:

- ripartire utili e/o acconti sugli utili non effettivamente conseguiti, ovvero destinati per legge a riserva, nonché ripartire riserve che per legge non possono essere ripartite;

- acquistare o sottoscrivere quote della Società, ovvero di eventuali controllanti, fuori dai casi previsti dalla legge con lesione dell'integrità del patrimonio sociale;

- effettuare riduzioni di capitale sociale, fusioni e/o scissioni, in violazione delle disposizioni di legge a tutela dei soci o creditori;

- ripartire i beni sociali tra i soci in danno dei creditori;

- alterare in modo fittizio, con qualsivoglia operazione societaria, il capitale sociale.

Al fine di prevenire la commissione di uno degli illeciti indicati all'interno della presente Parte Speciale, deve essere sempre assicurato:

- il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo previsto dalla legge, sia di carattere interno, sia di carattere esterno, sulla gestione sociale;

- la tempestività, la correttezza e la completezza di tutte le comunicazioni previste per legge o regolamento;

- la libera e corretta formazione della volontà;

- la regolare formazione, tenuta e conservazione di tutta la rilevante documentazione societaria, contabile e fiscale: a tal fine è fatto espresso divieto di tenere comportamenti che, mediante il mancato tempestivo aggiornamento della documentazione, la mancata corretta conservazione o l'occultamento dei documenti impediscano, alle autorità ed agli organi pubblici di vigilanza di effettuare le dovute attività di controllo.

5. Principi specifici di comportamento e procedure di prevenzione dei rischi

Per tutte le operazioni relative alle attività sensibili, viene individuato il Responsabile Interno del procedimento che si identifica con il Responsabile della Direzione competente per la gestione dell'operazione considerata.

Il Responsabile Interno del procedimento è il diretto responsabile dell'operazione a rischio e deve garantire il rispetto delle regole di condotta, delle politiche, dei principi di comportamento e delle procedure aziendali; lo stesso, in particolare, può chiedere informazioni e chiarimenti a tutte le Direzioni aziendali e a tutti coloro che si occupano, ovvero si sono occupati, di alcuni aspetti dell'operazione a rischio.

Tutte le operazioni relative alle aree di attività sensibili individuate sono regolamentate dai seguenti protocolli comportamentali specifici di prevenzione e controllo:

- la formazione degli atti e delle decisioni necessarie per adempiere alle obbligazioni tributarie, ed alla formazione delle dichiarazioni, deve essere sempre ricostruibile;

- i documenti inerenti le attività della Società devono essere sempre archiviati e conservati a cura della Direzione competente e con modalità tali da non permetterne la modificazione successiva, se non dandone specifica evidenza e consentendone l'accesso soltanto ai soggetti competenti, secondo le normative interne, e agli organi di controllo; l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate (ed eventualmente all'Organismo di Vigilanza);

- nell'impiego delle proprie risorse finanziarie la Società si avvale solo di intermediari

finanziari e bancari sottoposti ad una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea; tutti i pagamenti o le transazioni finanziarie devono essere effettuati esclusivamente tramite intermediari autorizzati, in modo che ne sia garantita sempre la tracciabilità sulla base di idonea documentazione.

I documenti fiscali, sia attivi che passivi, devono sempre avere una ragione giuridica reale e documentabile, allegando al documento fiscale l'atto giuridico sottostante.

6. *Flussi informativi in favore dell'OdV*

Al fine di fornire all'Organismo di Vigilanza gli strumenti per esercitare le attività di monitoraggio e di verifica puntuale della efficace esecuzione dei controlli previsti dal presente Modello e, in particolare, dalla presente Parte Speciale, nelle procedure sono descritti i flussi informativi che devono essere assicurati al predetto Organismo, in conformità a quanto disposto nella Parte Generale del Modello medesimo.

Tutti i soggetti interessati sono tenuti a comunicare il manifestarsi del singolo evento cui sono legati i rischio-reato ed i controlli attesi.

Lo strumento di comunicazione è rappresentato prevalentemente dall'e-mail da inviarsi all'indirizzo odv.scaranofusca@libero.it con la specificazione nell'oggetto del *reference* del flusso informativo cui si riferisce la comunicazione medesima.