Rangers S.r.l.

Modello di organizzazione gestione e controllo

RIFERIMENTI DI REVISIONE	
NUMERO REVISIONE	DATA
0. Versione originaria	03.12.2012
1. Prima revisione	15.10.2014
2. Seconda revisione	10.06.2015
3. Terza revisione	20.07.2020
4. Quarta revisione	09.11.2023

INDICE

1. PERCHÉ L'ADOZIONE DI UN MOG: IL D.LGS. 231/2001 5
A. LA RESPONSABILITÀ D'IMPRESA DI CUI AL D.LGS. 231/01 5
B. LA GIURISPRUDENZA: IL MOG COME ESIMENTE 6
Idoneità dei modelli 7
Il sistema dei controlli 8
Organismo di Vigilanza – Compiti (rinvio) 9
C. IL MOG: SOGGETTI E REATI 10
FATTISPECIE OBIETTIVA: AUTORI 11
Soggetti in posizioni apicali 11
Soggetti sottoposti all'altrui vigilanza 12
Onere probatorio 12
FATTISPECIE OBIETTIVA: INTERESSE O VANTAGGIO 14
FATTISPECIE OBIETTIVA: I REATI PRESUPPOSTO 15
Reati commessi all'estero 16
Individuazione dei reati rilevanti: metodo di analisi 16

2. IL MODELLO DELLA SOCIETÀ RANGERS S.R.L. 16
A. DESTINATARI DEL MODELLO 17
B. STRUTTURA DEL MODELLO 17
C. ANALISI DEL SISTEMA DI RISCHIO PRELIMINARE ALL'ADOZIONE DEL MODELLO 19

3. IDENTITÀ E STRUTTURA DELLA SOCIETÀ 19
A. SISTEMA DI GOVERNANCE 20
Organigramma 21
Presidente del CdA 21
AmministratorI DelegatI 21
TITOLARE DI LICENZA DI PUBBLICA SICUREZZA 21
Al Titolare di licenza di Pubblica Sicurezza compete la gestione, in nome e per conto della Società, dell'attività di vigilanza e trasporto. 21
RISK MANAGER 21
procuratori 21
DATA PROTECTION OFFICER (DPO) 21
Sindaco Unico 22
RESPONSABILE ANTIRICICLAGGIO 22
Sistema organizzativo 22
Datore di lavoro per la sicurezza 22
Responsabile Servizio Protezione e Prevenzione (RSPP). 23
La Direzione Amministrazione, Finanza e Controllo CORPORATE 23
La Direzione commerciale 23
FUNZIONE OPERAZIONI 23
Funzione acquisti Corporate 24
DIREZIONE CONTROLLO E RECUPERO CREDITI 24
Funzione It CORPORATE 24
DIREZIONE SISTEMI DI SICUREZZA E INNOVAZIONE 24
FUNZIONE ORGANIZZAZIONE AZIENDALE 24
DIREZIONE VIGILANZA CORPORATE 24
SERVIZI DI VIGILANZA 25

B. STATO DELLE PROCEDURE E OBIETTIVI PERSEGUITI CON L'ADOZIONE DEL MODELLO 25
C. SISTEMA DI DELEGHE E PROCURE 26
Principi generali *26*
Deleghe: criteri di attribuzione *26*
Procure: criteri di attribuzione *27*
Modalità di esercizio di Deleghe e Procure *27*

4. SISTEMA NORMATIVO INTERNO 28
A. EMANAZIONE DELLA NORMATIVA AZIENDALE 28
B. IL CODICE ETICO 28
D. C. ORGANISMO DI VIGILANZA 29
Nomina e durata *29*
Requisiti di professionalità *29*
Requisiti, recesso e cause di revoca *30*
Autonomia finanziaria *32*
Autonomia funzionale *32*
Compiti e attività *33*
Obblighi informativi dell'Organismo diVigilanza *35*
Obblighi informativi verso l'Organismo diVigilanza *36*

5. SEGNALAZIONI DI ILLECITI DA PARTE DEI DIPENDENTI 37
Definizioni *38*
Principi generali *39*
Oggetto e campo di applicazione *40*
Procedura di Segnalazione *40*
Invio delle segnalazioni 41
Istruttoria 43
TUTELA DEL SEGNALANTE E OBBLIGHI DI RISERVATEZZA *43*
Sanzioni e provvedimenti consequenziali *44*
Conservazione della documentazione *45*

6. IL REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI (GENERAL DATA PROTECTION REGULATION). 45

7. SISTEMA DISCIPLINARE 48
FUNZIONE DEL SISTEMA DISCIPLINARE *48*
informazione *48*
REQUISITI DEL SISTEMA DISCIPLINARE *48*
destinatari *49*
COMPORTAMENTI SANZIONABILI *49*
criteri di scelta delle sanzioni *50*
TIPOLOGIE DI SANZIONI APPLICABILI *50*
Sanzioni nei confronti dei soggetti apicali 50
Sanzioni nei confronti dei soggetti subordinati 51
Sanzioni nei confronti dei Terzi 52
modalitÀ DI IRROGAZIONE DELLE SANZIONI *53*

8. SISTEMA DI FORMAZIONE E DIFFUSIONE DEL MODELLO 54
Informazione del personale/ Diffusione del modello 54
Formazione del personale 55

1. PERCHÉ L'ADOZIONE DI UN MOG: IL D.LGS. 231/2001

A. LA RESPONSABILITÀ D'IMPRESA DI CUI AL D.LGS. 231/01

Il "Modello di organizzazione, gestione e controllo" di cui al D.lgs.231/2001 rappresenta la più significativa concretizzazione giuridica nell'ordinamento interno dell'esigenza, sottesa alla cd. *compliance* aziendale, della conformità alle prescrizioni normative. Espressione di un principio in sé elementare: le imprese nel perseguimento dei loro legittimi scopi utilitaristici non devono sfruttare o incorrere in condotte vietate, violando il dovere generale di non procurare danni a singoli individui e alla collettività.

In un sistema normativo sempre più improntato ai controlli e ai protocolli di prevenzione, tale esigenza viene calata all'interno di un preciso *frame* tecnicistico: il rispetto della legalità non si ottiene solo con la minaccia di sanzioni, ma anche e soprattutto attraverso un'efficace prevenzione endo-societaria, fatta di politiche, modelli gestionali, procedure decisionali e presidi di monitoraggio e di sorveglianza.

Volgendo lo sguardo al canone costituzionale di cui all'art. 27, comma 1, della Costituzione, il legislatore ha improntato la responsabilità degli enti da reato, ancorché formalmente etichettata come *amministrativa,* a un modello di imputazione strutturalmente assimilabile a quello penale *colposo*, in quanto fondato sulla nozione, del tutto normativa, di *colpa di organizzazione.* È tuttavia prevista una differenziazione di regime probatorio a seconda che il reato base sia stato commesso da soggetti di vertice dell'organizzazione o loro sottoposti.

Il nucleo del rimprovero mosso all'ente per i reati commessi nel suo interesse o a suo vantaggio da soggetti espressamente indicati dal legislatore risiede esattamente in un ***deficit* oggettivo di organizzazione in chiave preventiva**.

L'adozione e l'efficace attuazione di un Modello di Organizzazione e Gestione, idoneo a prevenire reati fra quelli legislativamente indicati, è, pertanto, momento fondante il dovere di organizzazione dell'ente e quindi fattore determinante per escluderne la sua rimproverabilità.

Inoltre, con il D.lgs. 231/2001[1], la corretta organizzazione interna in funzione della prevenzione dei fatti penalmente rilevanti non è più solo *munus* delle persone fisiche che dirigono l'ente (delle sue posizioni apicali), ma è divenuta parametro essenziale per misurare l'oculatezza della società in

[1]Per incentivare gli Enti ad assumere moduli comportamentali virtuosi, il decreto legislativo ha coniato, prendendo spunto dai *complianceprograms*nordamericani, un paradigma di tipo **punitivo – premiante:** minaccia di sanzioni rigorose (pecuniarie, ablative, interdittive e reputazionali) e contestuale promessa di esenzione dalla responsabilità nel caso di adozione ed efficace attuazione *ante factum* di un idoneo programma di prevenzione del rischio – reato.

quanto tale nel prevenire le proiezioni offensive prevedibili della propria attività. Da ciò consegue che è il complessivo funzionamento dell'ente rispetto al reato a dover essere valutato su questo piano, alla stregua di uno *standard* di diligenza verosimilmente più severo di quello richiesto per la persona fisica, considerate le maggiori capacità cognitive e di intervento che ha l'organizzazione come soggetto pluripersonale, rispetto all'individuo isolato.

Gli elementi fondamentali del Modello di Organizzazione – come detto, indispensabile strumento precauzionale individuato dal legislatore per prevenire la commissione di reati – sono indicati dagli artt. 6 e 7 D.lgs.231/01, che da un lato richiedono l'*idoneità* dello stesso e dall'altro tracciano il perimetro della regola modale che l'ente sarà chiamato a creare affinché l'attività di impresa resti entro la soglia del "rischio permesso". In tal modo la legge fornisce delle clausole generali che funzionano come parametri cui avere riguardo per ottenere indicazioni di massima che dovranno poi essere concretizzate di volta in volta in relazione alle singole esigenze degli enti con riferimento alle loro attività e organizzazioni.

In sintesi: la verifica giudiziale di idoneità del Modello di Organizzazione adottato va a testare la conformità delle regole precauzionali (cristallizzate nei diversi protocolli operativi) rispetto alle migliori conoscenze, consolidate e condivise nel momento storico in cui è commesso l'illecito, in ordine ai metodi di neutralizzazione o di minimizzazione del rischio tipico.

B. LA GIURISPRUDENZA: IL MOG COME ESIMENTE

Per giurisprudenza costante, la società che abbia omesso di adottare e correttamente applicare un Modello di organizzazione, gestione e controllo, non è responsabile del reato presupposto commesso dal titolare di una posizione verticistica (articolo 5, par. 2) solo se il colpevole ha agito nell'interesse esclusivo proprio o di terzi (Cass. pen., sez. VI, 9 luglio 2009, n. 36083). Nondimeno, in una recente sentenza la Corte di Cassazione ha ritenuto sussistente la responsabilità da reato dell'ente anche qualora l'autore del reato presupposto abbia agito per un interesse prevalentemente proprio[2] (Cass.pen., sez. VI, 25 settembre 2018 n. 54640).Al tempo stesso, la mera adozione di un Modello (articoli 6-7 del decreto) non è sufficiente. È stato così chiarito come il sistema di *compliance* adottato da un'azienda deve essere dotato di strumenti in grado di prevedere la valutazione dei rischi nei settori di attività, e in modo da verificare, *inter alia*, gli elementi "sintomatici" dei reati (*e.g.* presenza di conti correnti all'estero; utilizzo di intermediari stranieri che rendono difficile individuare la provenienza del pagamenti; il calendario dei pagamenti legati alle gare d'appalto cui partecipa la società) (Tribunale di Milano, sez. XI in funzione di giudice del Riesame, ordinanza 28 ottobre 2004). In sintesi, l'adozione di un sistema di prevenzione, la cui effettività trova un limite solo nell'elusione fraudolenta (non agevolata da un difetto di controllo) (Cass. pen. sez. V, 18 dicembre 2013 n. 4677), rende non rimproverabile all'ente la realizzazione dell'illecito consumato da un soggetto

[2] In motivazione, la Corte ha ritenuto sussistente un marginale interesse della società rispetto alla condotta corruttiva dell'imputato, da questi realizzata principalmente per tutelare la sua immagine all'interno della società, ma comunque suscettibile di consentire all'ente di evitare l'irrogazione di penali e sanzioni, pur se di minima consistenza.

formalmente deputato a incarnarne la politica d'impresa (funzione esimente del modello). Recente giurisprudenza (Sent. Cass., Sez. V, n. 43656 del 28 Novembre 2019) ha ribadito che nella valutazione della Responsabilità degli enti sia necessario: accertare preliminarmente l'esistenza di un Modello organizzativo e di gestione ex art. 6 del D.lgs 231/01; poi, nell'evenienza che il modello esista, andrà accertato che lo stesso sia conforme alle norme e, infine, che esso sia stato efficacemente attuato o meno in un'ottica di prevenzione, prima della commissione del fatto.

Va, poi, ricordato che il modello di prevenzione del rischio-reato svolge una ulteriore, importante funzione di natura riparatoria: la sua adozione (o il suo adeguamento) *post delictum* determina, ricorrendo altre condizioni (v. artt. 12 e 17 D.lgs. n. 231/2001), una ragguardevole riduzione della sanzione pecuniaria e l'inapplicabilità delle sanzioni interdittive. Il rilievo assegnato alle condotte di ravvedimento denota una significativa co-funzionalità con i criteri di ascrizione della responsabilità, atteso che viene valorizzato, in chiave special preventiva, il ruolo dei modelli in vista della minimizzazione del rischio-reato.

IDONEITÀ DEI MODELLI

La giurisprudenza ha, quindi, fornito alcune indicazioni sui requisiti presenti in un modello affinché possa essere ritenuto efficace.

La difficoltà principale nella redazione dei modelli, che comporta spesso la loro scarsa rilevanza processuale in chiave assolutoria, è dovuta alla loro astrattezza. Astrattezza che può essere ingenerata, a sua volta, dalla limitata tassatività delle fattispecie penali: la precisione dei modelli è direttamente proporzionale al grado di precisione del tipo criminoso. Di modo che un fatto di reato descritto "a maglie larghe" produrrà, a cascata, un modello ad ampio spettro. Da ciò discende la scelta, operata in questo modello, di operare una descrizione "fattuale" dei reati, così da ancorare la costruzione delle procedure non alla astratta previsione legale, ma alle tante modalità di realizzazione delle stesse.

Per la giurisprudenza, un modello **non può considerarsi idoneo** a prevenire i reati presupposto se:

- non includa una precisa individuazione dei settori di attività all'interno dei quali potrebbero essere commessi i reati;
- rispetto alle aree sensibili non contenga protocolli, procedure e previsioni specifiche e concrete, e previsioni specifiche, procedure esattamente determinate e determinabili, regole individuate anche nella loro rigida sequenza e funzionalmente dirette a garantire il conseguimento di risultati precisi;
- individuate le aree di rischio, non stabilisca per ognuno di esse specifici protocolli di prevenzione che regolino "nel modo più stringente ed efficace possibile le attività pericolose";oppure,qualora previsti non si sanzionino le violazioni o non si provveda a un costante e periodico controllo di queste regole preventive;
- non vengano esplicitate le modalità di gestione delle risorse finanziare al fine di evitare

la commissione di reati;

- non si prevedano sanzioni disciplinari nei confronti dei soggetti che, per negligenza o imperizia, non abbiano saputo individuare ed eliminare violazioni del modello e/o la perpetrazione dei reati presupposto;
- non si prevedano procedure di ricerca e identificazione dei rischi quando sussistano già segnali di rischio;
- non si disciplini un obbligo per i soggetti interessati (dipendenti, direttore, amministratori della società) di riferire all'organismo di vigilanza notizie relative alla vita dell'ente, a pregresse violazioni del modello o alla consumazione di reati (fornendo concrete indicazioni sulle modalità attraverso le quali coloro che vengano a conoscenza di comportamenti illeciti possono riferire all'organo di vigilanza);
- non si prevedano attività di formazione sulle regole del modello che sia differenziata a seconda della categoria dei soggetti coinvolti;
- non si disciplini il contenuto dei corsi di formazione del personale, la frequenza, l'obbligatorietà della partecipazione;
- non si prevedano controlli di frequenza e di qualità sul contenuto dei programmi.

IL SISTEMA DEI CONTROLLI

Rilevante anche a fini esimenti è il sistema dei controlli.

Ai sensi dell''art.6, co.1, lett.b), un modello efficiente deve conferire il compito di vigilare sul funzionamento e sull'osservanza delle proprie regole a un organo dotato di autonomi poteri di iniziativa e controllo (OdV).

Una corretta conformità alla previsione legislativa presuppone la non subordinazione del controllante al controllato (Cass. pen., sez. V, n. 4677, 30 gennaio 2014, Impregilo). Il che trova conferma nel comma secondo dell'art. 6 che, alla lett. *d)*, prevede obblighi di informazione nei confronti dell'organo di vigilanza e, evidentemente, un autonomo esercizio del potere di vigilanza, che a sua volta è rafforzato dalla lett.*e)*, con un sistema cioè disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

L'efficacia del modello risiede nell'ampiezza dei poteri conferiti all'Organismo di Vigilanza, il quale deve potere ostacolare la commissione di attività illecite o lanciare un segnale d'allarme in presenza di condotte dei vertici che fanno presagire un reato.

Le indicazioni provenienti dalla giurisprudenza (Cass. Pen., Sez. V, n. 4677,30 gennaio 2014; Trib. Roma, 4 aprile 2003) sono critiche sulla scelta di attribuire il controllo a un organo monocratico, specie se dipendente dal presidente della società, perché inficerebbe la credibilità e l'autonomia dell'organo di controllo.

L'OdV deve avere competenze:

- ispettive,

- di analisi dei sistemi di controllo,

e, infine,

- giuridiche.

L'OdV deve essere oggetto privilegiato di una serie di flussi informativi, che garantiscano la base cognitiva su cui lo stesso organismo deve operare. Per ottenere questo risultato, è necessario prevedere obblighi informativi nei confronti dell'OdV, in capo ai responsabili delle aree a rischio reato, nonché la previsione di autonome sanzioni disciplinari per la violazione di detti obblighi (come detto in precedenza e come sarà sviluppato successivamente).

La circolazione delle informazioni è infatti elemento essenziale, perché senza il possesso di adeguate basi cognitive ogni forma di controllo è non solo impensabile ma, soprattutto, di scarsa efficacia.

Il moltiplicarsi dei soggetti destinatari delle informazioni circa eventuali segnali di allarme (c.d. *redflag*s), può costituire quindi un potenziale deterrente per operazioni opache.

In sintesi: il Modello organizzativo deve essere valutato per la sua concreta e specifica effettività sulla base di un approccio realistico al fenomeno societario.

La cd. «colpa di organizzazione» si concretizza nel caso in cui l'ente collettivo non abbia sviluppato o, comunque, non abbia efficacemente attuato un modello di organizzazione idoneo a scongiurare (*rectius:* ridotto il rischiodi verificazione di*)* fatti-reato del tipo di quello realizzatosi effettivamente: non si sia dotato, cioè, di un *complianceprogram*, che sia, concretamente e sostanzialmente in grado di *minimizzare* i rischi di reato *ex* art.24.e ss. D.lgs. 231/01 (Trib. Milano, ordinanza del 20 settembre 2004).La responsabilità degli enti può dunque essere definita come una vera e propria responsabilità da colpa di organizzazione, caratterizzata dal malfunzionamento della struttura organizzativa dell'ente, la quale dovrebbe essere volta -mediante adeguati modelli- a prevenire la commissione di reati (Cass. Pen., Sez. IV, sentenza n. 38363 del 2018). Le Sezioni Unite hanno infatti al riguardo affermato che, in tema di responsabilità da reato degli enti, la colpa di organizzazione, da intendersi in senso normativo, è fondata sul rimprovero derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione dei reati previsti tra quelli idonei a fondare la responsabilità del soggetto collettivo, dovendo tali accorgimenti essere consacrati in un documento che individua i rischi e delinea le misure atte a contrastarli (Cass. SS.UU., sentenza n. 38343 del 2014).

ORGANISMO DI VIGILANZA – COMPITI (RINVIO)

Ai sensi dell'art 6 comma 1 lettera b) l'Organismo di vigilanza è l'organo di controllo del modello ed è responsabile dello svolgimento delle seguenti attività:

- curare l'attuazione del modello e in particolare la corretta introduzione e applicazione dei protocolli;
- vigilare sull'osservanza, funzionamento e aggiornamento del modello ai sensi del D.lgs.231/2001 e senza interferire con le competenze del Sindaco Unico;

- curare l'interpretazione nonché il rispetto delle disposizioni del Codice Etico, del modello e dei regolamenti, degli ordini di servizio e delle procedure aziendali previste in attuazione dello stesso;
- aggiornare e adeguare periodicamente il Modello al mutare di elementi **endogeni** della società (es. modifiche organizzative, poteri di firma, nuove attività);
- aggiornare e adeguare periodicamente il Modello al mutare di elementi **esogeni** della società (es. introduzione di nuovi reati nel D.lgs.231/01, chiarimenti derivanti dalla giurisprudenza dominante, decisioni di merito in ordine all'applicazione dei Modelli);
- riferire periodicamente al CdA, al Sindaco Unico e al Presidente della Società in merito allo stato di attuazione e all'operatività del Modello;
- segnalare al CdA, per gli opportuni provvedimenti, le violazioni del Modello e del Codice Etico.

C. IL MOG: SOGGETTI E REATI

La colpevolezza della società troverebbe fondamento in un «fatto» (talvolta anche fenomenologicamente) omissivo: il non avere impedito, o, se si preferisce, l'avere agevolato la commissione di un reato-presupposto da parte di persone fisiche inserite nell'organigramma aziendale, in conseguenza dell'inottemperanza *tout court,* oppure della trascurata – o, peggio, posticcia – ottemperanza, dell'*onere/obbligo* di auto-organizzarsi in modo da contenere il rischio d'illegalità penale.

Il Modello organizzativo, o meglio la sua assenza (o inidoneità, o inefficacia, Cass. Pen., Sez.VI, 9luglio2009, n.36083, *Mussoni e altri*) integra la *fattispecie subiettiva* dell'illecito dell'ente, radicandone la responsabilità «da reato» in presenza degli ulteriori e pregiudiziali presupposti obiettivi:

- Un fatto tipico e antigiuridico *ex* artt. 24 ss.D.lgs.cit.,
- Commesso nel suo interesse o a suo vantaggio,
- Da parte di un intraneo – persona fisica.

L'imputazione "soggettiva" della responsabilità all'ente richiede che si accerti la violazione di una regola di corretta organizzazione e gestione idonea a prevenire la commissione del reato ("di reati del tipo di quello verificatosi", nelle parole dell'art. 6). Da ciò discende, per costante giurisprudenza, che perché sia superato il vaglio di adeguatezza non debba aversi riguardo all'intero Modello, ma ci si rapporti con lo specifico reato *sub iudice*. Il giudizio da superare è un giudizio concreto e relativo, anziché astratto ed esteso al modo di essere dell'intera organizzazione (preventiva). Pertanto, la verifica giudiziale di idoneità del modello penal-preventivo adottato dall'ente si risolve in un giudizio normativo volto a controllare, non tanto l'eventuale violazione di precise regole cautelari di fonte legislativa (o secondaria), quanto la conformità delle regole prevenzionali auto-normate dall'ente alle migliori conoscenze consolidate e condivise nel momento storico in cui è commesso l'illecito, in ordine ai metodi di neutralizzazione o di minimizzazione del rischio tipico.

FATTISPECIE OBIETTIVA: AUTORI

Quanto alla **fattispecie obbiettiva**, l'art. 5 del Decreto 231/01 stabilisce che la responsabilità per l'azienda può nascere da reati commessi da:

- persone che rivestono funzioni di rappresentanza,di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (vertice aziendale);
- persone sottoposte alla direzione o alla vigilanza dei soggetti di cui al punto precedente (responsabili).

SOGGETTI IN POSIZIONI APICALI

Pur avendo la normativa utilizzato un criterio funzionale per l'individuazione degli apici (amministrazione, direzione, rappresentanza), il legislatore ha espressamente equiparato, ai soggetti che formalmente esercitano tali funzioni, le persone che "esercitano, anche di fatto, la gestione e il controllo dell'ente stesso (art. 5 comma 1, lett. a Decreto 231/01). Si osserva, tuttavia, che l'esercizio di fatto è rilevante solo se si esercitano cumulativamente i poteri di gestione e di controllo "volendosi includere tra i vertici solo quei soggetti che esercitano un penetrante dominio sull'ente" (Relazione ministeriale al decreto legislativo 231/2001).

In letteratura e in giurisprudenza è stato affermato che:

- ✓ Il concetto di **rappresentanza** dell'ente richiama il potere di formare, ricevere e manifestare verso l'esterno la volontà dell'ente in relazione ad atti negoziali;
- ✓ Il concetto di **amministrazione** della società può essere interpretato come il potere di gestione e controllo *delle risorse materiali dell'ente*;
- ✓ Il concetto di **gestione** richiama il potere di gestione e controllo del personale dell'ente.

Per l'individuazione del soggetto apicale, dunque, ciò che conta, al di là di una investitura formale, è lo svolgimento in concreto delle funzioni o mansioni tipiche di chi amministra e/o gestisce l'ente, ciò valendo sia nel caso (del tutto marginale) in cui sia rinvenibile una nomina viziata o implicita, sia nell'ipotesi (ben più ricorrente) in cui l'attività gestoria venga svolta in assenza di qualsivoglia atto di nomina del competente organo sociale.

Con particolare riferimento a specifiche figure, dalla giurisprudenza in materia si ricava che:

l'Amministratore Unico rientra certamente nella definizione di soggetto apicale (Cassazione, II sez. sentenza del 30 gennaio 2006, n. 3615) – ruolo allo stato non previsto;

i componenti del Consiglio di Amministrazione svolgono *ex lege* funzioni di gestione e di controllo delle imprese; pertanto, non sussistono dubbi sulla riconducibilità delle funzioni svolte dal soggetto posto in posizione apicale. Pare si possa giungere alla medesima conclusione qualora vi sia un Amministratore Delegato, poiché i membri del C.d.A. rimangono titolari di un potere di controllo che può arrivare sino all'avocazione a sé del compimento di operazioni delegate;

l'Amministratore Delegato, in quanto organo chiamato a esercitare funzioni proprie del Consiglio di Amministrazione, rientra a pieno titolo nel novero dei soggetti apicali, limitatamente ai poteri allo stesso conferiti. In ogni caso occorrerà verificare di volta in volta se l'azione delittuosa rientra nelle attribuzioni devolute all'Amministratore Delegato o se la condotta contestata non si sia generata in relazione a una operazione, seppur rientrante nella delega, avocata a sé dal Consiglio di Amministrazione;

il Direttore Generale, la cui figura è disciplinata dall'art. 2396 c.c. senza fornire una definizione intrinseca delle mansioni e delle funzioni ricoperte, ma prevendendo che le disposizioni che regolano la responsabilità degli amministratori si applichino anche ai direttori generali nominanti dall'assemblea o per disposizione dello statuto. Sebbene non sempre la giurisprudenza sia concorde (Cass. civ., sez. I, 5 dicembre 2008, n. 28819), si può comunque affermare che il Direttore Generale nominato formalmente rientri nella nozione di soggetto apicale - ruolo allo stato non previsto;

le persone che dirigono unità periferiche dotate di autonomia finanziaria e funzionale: la figura esemplare nell'ambito della specifica organizzazione di Rangers S.r.l.è quella del Direttore di Divisione; rientrano tra questi anche i **preposti a una stabile organizzazione come per esempio i Responsabili di Filiale,** destinatari di una forte autonomia gestionale e perciò sottratti al controllo delle sedi centrali. In ogni caso, in questi ambiti molto dipenderà dal risultato dell'accertamento probatorio;

le figure del datore di lavoro, del dirigente e del preposto, tali soggetti sono individuati dal T.U. in materia di sicurezza del lavoro quali destinatari, a vario titolo, di posizioni di garanzia.

SOGGETTI SOTTOPOSTI ALL'ALTRUI VIGILANZA

La seconda categoria di soggetti disciplinata dall'art. 5 ha la funzione di individuare, per il tramite di una sorta di clausola residuale, tutte le altre persone fisiche, diverse dagli apicali, che prestano la propria attività lavorativa nell'interesse dell'ente.

Da subito deve essere sottolineato come la commissione di un reato da parte dei sottoposti alla direzione o alla vigilanza dei soggetti apicali coinvolge la responsabilità dell'ente, diversa, tuttavia, sarà la prova liberatoria concessa all'ente per esimersi dalla responsabilità.

Il criterio di imputazione delle condotte illecite dei sottoposti risiede nella presunzione che, in linea di massima, gli stessi agiscano in funzione delle direttive aziendali e che, sotto il profilo oggettivo, gli stessi operino nell'interesse dell'ente.

La definizione fornita dal Decreto non è di carattere formale ma oggettivo-funzionale e, pertanto, non è necessario che i sottoposti abbiano con l'ente un rapporto di lavoro subordinato, dovendosi ricomprendere in questa nozione anche quei prestatori di lavoro che, pur non essendo "dipendenti" dell'ente, abbiano con esso un rapporto tale da far ritenere che sussiste un obbligo di vigilanza da parte dei vertici dello stesso.

ONERE PROBATORIO

In nessun caso la società, sia che a commettere il fatto di reato sia un soggetto ai vertici dell'ente sia che l'agente sia sottoposto all'altrui direzione, risponde di quanto realizzato a titolo di responsabilità oggettiva "*essendo previsto necessariamente per la sua configurabilità, la sussistenza della cosiddetta «colpa di organizzazione» della persona giuridica*" (Cass. pen., sez. VI, 18.02.2010, n. 27735; in senso conforme: Cass. pen., sez. III, 7.06.2011). Tuttavia, nelle due ipotesi in precedenza descritte il criterio dell'immedesimazione organica che lega il soggetto all'ente collettivo e che, conseguentemente, consente di ascrivere un'azione del singolo alla società, si atteggia in maniera diversa a seconda che il soggetto rivesta una posizione apicale o che quest'ultimo sia sottoposto. La scelta legislativa è facilmente intuibile: alcuni soggetti sono inseriti a tal punto nelle strutture decisionali degli enti collettivi, per cui si presume che le azioni intraprese siano espressione della politica d'impresa. La distinzione, in effetti, rispecchia la macro-dicotomia criminologica tra illeciti dell'ente espressivi della politica di impresa (in cui le attività criminose corrispondono normalmente a decisioni di vertice e quindi a reati commessi dai soggetti apicali) e illeciti che costituiscono il risultato della carenza di controllo da parte degli apici o in generale della disorganizzazione aziendale – in cui i reati sono commessi da subordinati o addirittura rimane ignoto l'autore (art. 8).

Così, una volta accertata la commissione di determinati reati da parte delle persone fisiche che esercitano funzioni apicali, i quali abbiano agito nell'interesse o a vantaggio delle società, incombe sugli enti l'onere, con effetti liberatori, di dimostrare di aver adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi (Cass. pen. Sez. III, sentenza n. 18842 del 2019).In tal caso, quindi, la società, per andare esente da responsabilità, avrà un onere probatorio molto più gravoso.

In caso di reato commesso da un soggetto in posizione apicale, la società non risponde se prova che (art. 6, comma 1, D.lgs. 231/01):

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

Il dato normativo è chiaramente nel senso di un'inversione dell'onere probatorio, in virtù della particolare qualità degli autori materiali del reato. La prova degli elementi atti a escludere la responsabilità dell'ente è, pertanto, a carico dell'ente stesso. Sussiste quindi una presunzione di responsabilità fondata sul fatto che i soggetti apicali di regola esprimono la politica dell'ente; ove ciò non accada, dovrà essere la società stessa a dimostrare la sua estraneità, e potrà farlo soltanto provando la sussistenza di una serie di requisiti tra loro concorrenti.

In particolare, nel caso previsto dall'art. 5, comma 1, lett. a del Decreto, l'ente non risponderà della commissione del reato da parte di un soggetto apicale se proverà che, oltre ad avere adottato ed efficacemente attuato il Modello, ha posto in essere, attraverso l'Organismo di controllo al fine nominato, una "effettiva vigilanza" e che le persone fisiche hanno commesso il reato eludendo fraudolentemente il sistema di prevenzione in essere.

In giurisprudenza si rinvengono precedenti in cui, nonostante la commissione di un reato da parte degli apici, l'ente è andato esente da responsabilità avendo dato la dimostrazione di aver adottato tutte le misure organizzative e funzionali di precauzione e di controllo per evitare il comportamento illecito. (Tribunale Milano, ordinanza del 17.11.2009, cd. caso Impregilo; TAR Trento – Trentino Alto Adige, sez. I, 2.11.2011, n. 275).

In dottrina e in giurisprudenza per rappresentare l'apice che elude fraudolentemente il Modello si è fatto ricorso alla figura del cd. *amministratore infedele*, cioè di chi agisca contro l'interesse dell'ente. (Trib. Milano, ordinanza 17.11.2009; Cass. pen., sez. VI 9.07.2009 n. 36083).

Rimane, in ogni caso, la necessità per l'ente di dimostrare di aver adottato, attraverso gli organi preposti, procedure atte a evitare la commissione di fatti di reato da parte dei vertici aziendali, di aver nominato un organismo con il compito di vigilare sul sistema di prevenzione adottato e che il citato organismo abbia efficacemente vigilato.

Nel caso di un reato commesso dai sottoposti all'altrui direzione, l'onere della prova di dimostrare la *colpevolezza* dell'ente ritorna in capo all'autorità procedente, poiché l'ente vedrà soddisfatto il suddetto intervento dimostrativo nella fase di accertamento attraverso la sola prova di aver adottato il Modello e di aver vigilato su di esso. Non è dunque richiesta la *probatio* diabolica dell'elusione fraudolenta come nel caso degli apicali. È esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione e di gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. E nel caso di soggetti "sottoposti" l'onere probatorio (circa l'idoneità del Modello) sarà a carico dell'accusa, posto che l'art. 7, al comma 2, introducendo una presunzione *iuris et de iure*, esclude gli obblighi di direzione e di vigilanza, fonte della responsabilità dell'ente, nel caso di reati commessi da soggetti eterodiretti, in caso di preventiva adozione di un modello di organizzazione, gestione e controllo (Tribunale Milano, ordinanza 26.06. 2007).

FATTISPECIE OBIETTIVA: INTERESSE O VANTAGGIO

Ulteriore elemento della **fattispecie obiettiva** è dato dalla sussistenza dell'**interesse o vantaggio** dell'ente nel reato commesso. Il legislatore ha così inteso delimitare i confini della responsabilità dell'ente individuando nell'interesse e vantaggio gli indici della riferibilità della condotta del singolo all'ente. Si presume, infatti, che la condotta della persona offesa sia una manifestazione di una politica d'impresa orientata alla violazione delle regole di diritto. Con tale locuzione il D.lgs. 231/01 ha inteso rafforzare l'idea della immedesimazione organica, che, invero, funge da architrave dell'intero impianto normativo: la commissione del reato da parte dell'organo – persona fisica nell'interesse o vantaggio dell'ente è in grado di escludere la responsabilità dell'ente medesimo rispetto a tutti quei fatti che siano estranei all'organizzazione; fatti, vale a dire, che non appartengono

alla compagine sociale o non sono alla stessa in alcun modo riconducibile.

Tuttavia, ai sensi del secondo comma dell'art. 5, l'ente non risponde nel caso in cui i soggetti, siano essi apicali o sottoposti all'altrui direzione o vigilanza, abbiano agito "nell'interesse esclusivo dell'ente". Si tratta di una causa di esclusione della responsabilità oggettiva che attenua il generale principio della immedesimazione organica. In senso opposto, vale a dire in caso di automatismo in ogni caso della responsabilità dell'ente si sarebbe scivolati verso un modello di responsabilità oggettiva (in questo senso, Tribunale di Milano, sentenza del 28 aprile 2008).

L'ente sarà chiamato a rispondere, inoltre, anche qualora il fatto di reato, pur non essendo espressione di una politica aziendale, si sia realizzato a causa di un difetto nel sistema di controllo e di gestione, il quale deve essere volto alla prevenzione di comportamenti potenzialmente criminali.

Per giurisprudenza maggioritaria i criteri di imputazione oggettiva, rappresentati dall' "interesse o vantaggio", sono alternativi e concorrenti tra loro, in quanto il criterio dell'interesse esprime una valutazione teleologica del reato, apprezzabile "*ex ante*", cioè al momento della commissione del fatto e secondo un metro di giudizio marcatamente soggettivo, mentre quello del vantaggio ha una connotazione essenzialmente oggettiva, come tale valutabile "*ex post*", sulla base degli effetti concretamente derivati dalla realizzazione dell'illecito (Cass., SSUU, sentenza del 24 aprile 2014 n. 38343; cfr. Sez.V, 28 novembre 2013, n. 10265)

FATTISPECIE OBIETTIVA: I REATI PRESUPPOSTO

Il legislatore del 2001 ha perimetrato selettivamente a livello normativo generale e astratto il raggio di azione della tipologia di responsabilità penale di impresa attraverso una enumerazione tassativa delle fattispecie incriminatrici da cui può scaturire la responsabilità dell'ente, predefinendo quindi un *numerusclausus* non suscettibile di integrazione analogica. Le condotte illecite sono individuate dagli articoli 24 e ss. del D.lgs. 231/01. Come è noto, tuttavia, tale elencazione non è stata frutto di un organico e completo intervento espressivo di un chiaro piano di contrasto alla criminalità di impresa in grado di indicare a monte tutte le fattispecie tipiche ascrivibili alla politica aziendale. Al contrario, la scelta è stata quella di una "formazione progressiva" di tale catalogo, con una successiva e continua estensione delle sue dimensioni in modo da disegnare un inventario in continua crescita[3].

[3] Il legislatore ha previsto una disciplina sanzionatoria conseguente all'accertamento dell'illecito applicabile direttamente agli enti coinvolti nel procedimento penale. In particolare, sanzioni pecuniarie (artt. 10-12), sanzioni interdittive (artt. 13-17), confisca (art.19), pubblicazione della sentenza (art.20). Il sistema sanzionatorio è, alla luce di tale classificazione, contraddistinto da un carattere essenzialmente binario per cui da un lato si hanno sanzioni amministrative pecuniarie con carattere indefettibile (destinata a seguire sempre una sentenza di condanna) e dall'altro sanzioni interdittive applicabili solo ad alcune ipotesi tassativamente previste nei casi di particolare gravità.

REATI COMMESSI ALL'ESTERO

L'ente può essere chiamato a rispondere in Italia per i reati - contemplati dallo stesso D.lgs. n. 231/2001 - commessi all'estero (art. 4 D.lgs. n. 231/2001).

I presupposti su cui si fonda la responsabilità dell'ente per reati commessi all'estero sono:

(i) il reato deve essere commesso da un soggetto funzionalmente legato all'ente, ai sensi dell'art.5 comma 1 del d.lgs. n. 231/2001;

(ii) l'ente deve avere la propria sede principale nel territorio dello Stato italiano;

(iii) l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (pertanto nei casi in cui la legge prevede che l'autore - persona fisica - sia punibile secondo la legge italiana e, in quel caso, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso);

(iv) sussistendo i casi e le condizioni di cui ai predetti articoli del codice penale, nei confronti dell'ente non procede lo Stato del luogo in cui è stato commesso il fatto.

INDIVIDUAZIONE DEI REATI RILEVANTI: METODO DI ANALISI

Per la costruzione di un modello adeguato e idoneo al perseguimento delle finalità indicate dalla normativa di settore, i reati presupposto rilevanti sono stati individuati a seguito di una **mappatura del rischio** (vale a dire una individuazione di tutte le aeree sensibili), sulla cui base sono state specificate le attività in cui appare radicato il rischio di commissione di illeciti penali e le modalità operative attraverso le quali appare più ricorrente che vengano commessi reati. A tal fine:

- per giungere a individuare le attività sensibili, si è proceduto con una analisi, prevalentemente documentale, della struttura societaria e organizzativa della Società, svolta al fine di comprendere l'ambito in cui la Società opera e di identificare i processi aziendali oggetto dell'intervento. La raccolta della documentazione rilevante e l'analisi della stessa da un punto di vista sia tecnico-organizzativo sia legale ha permesso l'individuazione delle attività sensibili e una preliminare identificazione delle funzioni responsabili di tali attività;
- sono state analizzate le attività svolte e le vicende trascorse della Società, valutando se siano stati commessi reati in passato e le modalità attraverso le quali tali reati siano stati eventualmente realizzati;
- si è tenuto conto dell'evoluzione del quadro normativo, della giurisprudenza e della dottrina, nonché della prassi delle società italiane in relazione ai modelli.

2. IL MODELLO DELLA SOCIETÀ RANGERS S.R.L.

Il Modello è stato adottato dal Consiglio di Amministrazione di Rangers S.r.l. (di seguito anche denominata "la Società") con apposita delibera del 03 dicembre 2012, successivamente revisionato e aggiornato, da ultimo, il 09 novembre 2023.

Costituendo il presente Modello «atto di emanazione dell'organo dirigente», ai sensi dell'art. 6 co.1 lett.a) del Decreto, la competenza sulle sue eventuali successive modifiche e integrazioni spetta al Consiglio di Amministrazione.

Le modifiche di carattere formale al testo del Modello possono essere adottate dal Presidente del CdA, salva successiva comunicazione al Consiglio di Amministrazione.

Nella predetta delibera tutti i membri del Consiglio di Amministrazione hanno dichiarato di impegnarsi al rispetto del presente Modello.

Allo stesso modo il Sindaco Unico, presa visione del presente Modello, si è impegnato al rispetto dello stesso.

Data l'importanza di un'adeguata informazione dei destinatari del Modello, il documento, una volta approvato, deve essere oggetto di puntuale diffusione al personale, nonché ai fornitori, consulenti e *partner* della Società.

Il compito di curare, ove necessario, l'aggiornamento del Modello, proponendo al Consiglio di Amministrazione le opportune modifiche, e di vigilare sul funzionamento e sull'osservanza dello stesso, spetta allo Organismo interno di Vigilanza (qui di seguito "OdV").

A. DESTINATARI DEL MODELLO

Destinatari del Modello Organizzativo sono i soggetti in posizione "apicale"– compresi gli organi direttivi della Società (Consiglieri di Amministrazione, Procuratori)– nonché quelli sottoposti alla direzione o vigilanza degli "apicali", ai sensi dell'art. 5 del Decreto. Nell'una e nell'altra categoria, possono rientrare:

a) Personale formalmente inquadrato in organico sulla base di contratti di lavoro subordinato o a progetto;

b) Liberi professionisti formalmente inquadrati in organico: costoro, svolgendo un'attività coordinata e continuativa all'interno della Società, possono commettere reati "nell'interesse o a vantaggio" della Società. È dunque indispensabile che il Modello Organizzativo sia attuato anche nei loro confronti con le stesse modalità, in quanto compatibili, riservate ai lavoratori dipendenti: a tal fine, la Società adotta, nei contratti di collaborazione libero-professionale senza vincolo di dipendenza, specifica clausola di impegno al rispetto delle prescrizioni del Modello, con apposita previsione di sanzioni graduate in funzione della gravità della violazione.

Inoltre, sono da considerarsi Destinatari delle disposizioni di cui al presente Modello Organizzativo i consulenti e ogni altro soggetto che operi in nome e per conto della Società.

B. STRUTTURA DEL MODELLO

Il Modello redatto ai sensi del D.lgs. 231/01 è costituito da una Parte Generale e da una Parte Speciale. Nella presente Parte Generale vengono illustrate le componenti strutturali del Modello, ovvero:

- il sistema di *corporate governance*;
- il sistema di deleghe e procure;
- i Protocolli di conformità al D.lgs. 231/2001;
- il Codice Etico;
- i requisiti e le regole di funzionamento dell'Organismo di Vigilanza;
- la comunicazione e la formazione del personale sul Modello;
- il Sistema Disciplinare.

La Parte Speciale è, a sua volta, attualmente suddivisa in otto documenti di approfondimento:

- **Parte Speciale I, relativa a Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità;**
- **Parte Speciale II, relativa a Gestione degli approvvigionamenti;**
- **Parte Speciale III, relativa a Selezione, assunzione e gestione del personale;**
- **Parte Speciale IV, relativa a Gestione ed esecuzione dei servizi di vigilanza e trasporto;**
- **Parte Speciale V, relativa a Gestione degli adempimenti previsti in materia di sicurezza, salute sul lavoro e ambiente;**
- **Parte Speciale VI, relativa a Gestione della tesoreria, della formazione del bilancio e dei rapporti con i soci e con gli organi di controllo;**
- **Parte Speciale VII, relativa a Gestione delle infrastrutture tecnologiche e dei sistemi informativi;**
- **Parte Speciale VIII, relativa alla Gestione delle operazioni e degli adempimenti fiscali.**

Nell'ambito delle Part i Speciali, sono stati indicati:

- i processi a potenziale "rischio reato" e le relative attività sensibili;
- le funzioni e/o i servizi e/o gli uffici aziendali che operano nell'ambito delle aree a rischio reato o delle attività sensibili;
- i reati astrattamente perpetrabili;
- i presidi di controllo rilevanti nell'ambito delle singole aree di rischio;
- i principi di comportamento da rispettare al fine di ridurre il rischio di commissione dei reati;
- i flussi informativi con l'OdV;

- le modalità di conservazione della documentazione.

Considerata l'attività svolta, le Aree operative da considerare potenzialmente a rischio riguardano principalmente:

- relazioni con la PA., incluse partecipazioni a gare d'appalto, e scelta di consulenti/agenti e gestione dei rapporti con gli stessi in relazione a rapporti con la P.A.;
- rimborsi spese dipendenti;
- risorse umane, con particolare attenzione alla selezione delle guardie particolari giurate;
- contratti di consulenza;
- rapporti commerciali/acquisizione clientela;
- acquisti;
- gestione contenzioso e rapporti con organi giudiziari e autorità pubbliche di vigilanza;
- gestione finanziaria;
- amministrazione, contabilità e bilancio, con particolare attenzione a:
- adempimenti fiscali, contributivi, previdenziali;
- fatturazione;
- predisposizione dei dati per il bilancio;
- rendicontazione delle attività svolte, soprattutto verso la Pubblica Amministrazione;
- gestione assemblee;
- vigilanza;
- salute e sicurezza sul lavoro;
- servizi informatici, trasmissione di dati informatici.

C. ANALISI DEL SISTEMA DI RISCHIO PRELIMINARE ALL'ADOZIONE DEL MODELLO

Il presente Modello Organizzativo risulta formulato sulla base di una valutazione dell'assetto Aziendale in relazione ai profili di rischiosità di cui le relative Funzioni Aziendali risultano essere caratterizzate nell'espletamento delle normali attività.

Sulla base delle risultanze del documento denominato Risk Assessment (cui si fa rinvio per la riproduzione del Rischio Inerente alle attività aziendali e Rischio Residuo susseguente alla predisposizione del presente Modello) si sono predisposti i relativi protocolli operativi, congiuntamente alle esigenze Aziendali delle Funzioni specificamente coinvolte.

3. IDENTITÀ E STRUTTURA DELLA SOCIETÀ

Rangers S.r.l., società del Gruppo Battistolli, è stata costituita con l'obiettivo di operare prevalentemente nel settore della vigilanza.

I servizi erogati da Rangers S.r.l. si possono dividere nell'unica macro area dei servizi di vigilanza, in risposta alle esigenze sia del privato cittadino che delle attività commerciali ed industriali. Quali:

- Pattugliamenti fissi presso unità produttive, commerciali, residenziali e presso banche, Enti-Uffici Pubblici, musei, porti e aeroporti;
- Pattugliamenti mobili in zone residenziali, artigianali - industriali e commerciali con servizi di pronto intervento;
- Posti fissi di sorveglianza presso gli ingressi ed i punti prestabiliti di unità produttive, commerciali e residenziali ed in occasione di manifestazioni ed eventi di carattere pubblico e privato;
- Collegamenti in radiofrequenza tra il committente e la centrale operativa per il controllo e la gestione delle segnalazioni di allarme;
- Collegamento in videolento tra le strutture-clienti e le centrali operative per il controllo a distanza di particolari situazioni a rischio, come parcheggi, ingressi, locali adibiti a caveau, locali di banche per la sorveglianza interna;
- Servizi di antitaccheggio con guardie o videocontrollo per la repressione dei furti all'interno di ipermercati, autogrill, centri commerciali, depositi e grandi magazzini;
- Servizi di telecontrollo a distanza per la prevenzione dei rischi sui luoghi di lavoro e su locali pubblici (incendi, allagamenti, etc.); controlli delle uscite di sicurezza;
- Servizi di televigilanza per il controllo di beni storico-artistici in locali aperti o in musei-gallerie;
- Servizi di telesorveglianza dei flussi stradali ed autostradali, di tratti ferroviari e passaggi a livello, di cavalcavia e sottopassaggi;
- Controlli via satellite con sistema di localizzazione in tempo reale (Global Position System) di unità mobili in dotazione a clienti, nonché collegamenti con particolari complessi immobiliari dove la trasmissione satellitare (Discoverer) consente una più ampia sicurezza;
- Collegamenti per la gestione ed il controllo dei livelli (temperature, cicli produttivi, livelli idrici, etc.) di fabbriche, supermercati, centri di rilevazione idro-geologica;
- Collegamenti ARGOTEL per antintrusione; Collegamenti per la rilevazione-prevenzione degli incendi e delle fughe di gas;
- Monitoraggio a distanza degli accessi (aperture-chiusure), gestione- registrazione eventi in locali chiusi (aperture-chiusure casseforti, segnalazione antirapina, panico, etc.)
- Servizio di trasporto e scorta valori e servizi su apparecchiature automatiche, bancomat e casseforti, per il trasporto valori di denaro contante limitato a euro 100.000,00.
- Servizio scorta a beni trasportati con mezzi diversi da quelli destinati al trasporto valori, di proprietà di Rangers S.r.l. o di terzi.

La Direzione logistica dei servizi operativi e di sicurezza di Rangers S.r.l.è a Vicenza; le sedi operative sono collegate in rete e gestiscono indipendentemente l'attività in area locale.

A. SISTEMA DI GOVERNANCE

La Società è amministrata da un Consiglio di Amministrazione composto da 5 membri nominati dall'Assemblea ordinaria dei Soci. Tutti i componenti del CdA sono nominati per un periodo di tre esercizi e sono rieleggibili.

Al Consiglio di Amministrazione compete la gestione ordinaria e straordinaria della Società; esso può conseguentemente intraprendere qualsiasi azione che ritenga opportuna al fine del perseguimento dell'oggetto sociale della Società, a eccezione delle materie che, secondo la Legge o

lo Statuto vigente, sono espressamente attribuite alla competenza esclusiva dell'Assemblea dei Soci.

Il Consiglio di Amministrazione nomina gli Amministratori Delegati, nonché i procuratori, determinandone la durata, il contenuto e i limiti dei poteri delegati.

Il Sindaco Unico è l'organo di controllo contabile della Società che vigila come da legge sulla corretta amministrazione della Società, in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dagli amministratori e sul suo concreto funzionamento.

L'Assemblea dei Soci è competente a deliberare sulle materie alla stessa riservata dalla legge.

ORGANIGRAMMA

PRESIDENTE DEL CDA

Al Presidente, nominato dal Consiglio di Amministrazione, oltre ai poteri propri o derivanti dallo Statuto e dalla legge o conferiti dal Consiglio di Amministrazione, spetta la rappresentanza legale della Società dinanzi a terzi e agli organi giudiziari.

AMMINISTRATORI DELEGATI

Gli Amministratori Delegati sono nominati dal Consiglio di Amministrazione. Agli Amministratori Delegati spettano, oltre a ulteriori poteri conferiti dal Consiglio di Amministrazione, il compito di proporre le linee strategiche di sviluppo della Società.

TITOLARE DI LICENZA DI PUBBLICA SICUREZZA

AL TITOLARE DI LICENZA DI PUBBLICA SICUREZZA COMPETE LA GESTIONE, IN NOME E PER CONTO DELLA SOCIETÀ, DELL'ATTIVITÀ DI VIGILANZA E TRASPORTO.RISK MANAGER

Il *Risk Manager* individua e analizza i potenziali rischi in cui può incorrere l'Azienda per limitarne l'esposizione. L'incarico è affidato a un consulente esterno con apposito contratto.

PROCURATORI

I Procuratori designati con atto formale compiono attività in nome e per conto della Società con firma singola e disgiunta e con espresso potere di perfezionare i relativi atti, fermi restando i limiti ai poteri previsti nelle rispettive procure. In particolare, le procure sono state conferite in materia di Amministrazione e Finanza e gestione del Personale, con specifico riferimento al contenzioso.

DATA PROTECTION OFFICER (DPO)

Il DPO ha il compito e il ruolo di sorvegliare, attraverso gli strumenti di *accountability* di cui la società si è dotata, l'osservanza del Regolamento Europeo 679/16 (GDPR) in materia di protezione dei dati personali. Il ruolo è ricoperto da un consulente esterno, in possesso dei requisiti di autonomia e indipendenza richiesti alla figura di controllo.

SINDACO UNICO

Il Sindaco Unico ha il compito di:

- controllare l'amministrazione della Società e il suo corretto funzionamento;
- vigilare sull'osservanza delle norme di legge, dello Statuto, dei regolamenti e delle deliberazioni sociali, sulla corretta amministrazione, sull'adeguatezza degli assetti organizzativi e contabili della società.

RESPONSABILE ANTIRICICLAGGIO

Il Responsabile Antiriciclaggio ha il compito di garantire il rispetto complessivo della normativa antiriciclaggio. L'incarico è ricoperto da una figura di adeguata competenza e professionalità.

SISTEMA ORGANIZZATIVO

La Società è una S.r.l. organizzata mediante:

- sede Centrale con Direzioni/Funzioni Centrali;
- sedi operative;
- inserimento nell'ambito del Gruppo Battistolli.

I poteri e la rappresentanza sono delegati secondo un sistema ordinato di deleghe e procure.

Sono state poi individuate, in base all'attuale organigramma, le principali funzioni aziendali, di seguito riportate, ciascuna dotata di specifici poteri di controllo:

- *datore di lavoro per la sicurezza e suo delegato;*
- *responsabile Servizio Protezione e Prevenzione (RSPP);*
- *funzione commerciale;*
- *funzione operazioni;*
- *funzione controllo e recupero crediti;*
- *funzione sistemi di sicurezza e innovazione;*
- *funzione assistenza tecnico/commerciale;*
- *funzione fatturazione – Ufficio contratti*
- *direzione / funzione Risorse Umane Corporate;*
- *Direzione Acquisti Corporate;*
- *Direzione IT Corporate;*
- *Direzione Amministrazione e Finanza Corporate;*
- *Direzione organizzazione aziendale corporate*

DATORE DI LAVORO PER LA SICUREZZA

Il Datore di lavoro, nominato con apposita delega, svolge tutte le attività previste dall'art. 3 del D.Lgs. 81/08, al quale si rinvia. La società ha individuato anche, con apposita procura, un delegato di funzioni, ex art. 16 del D. Lgs. 81/08, al quale spettano tutti i controlli e le verifiche in materia di sicurezza sui luoghi di lavoro.

RESPONSABILE SERVIZIO PROTEZIONE E PREVENZIONE (RSPP).

Il RSPP svolge le attività previste dall'art.33 del D.Lgs. 81/08, al quale si rinvia.

LA DIREZIONE AMMINISTRAZIONE, FINANZA E CONTROLLO CORPORATE

La direzione amministrazione, finanza, pianificazione e controllo gestisce i sistemi e le risorse contabili al fine di garantire un adeguato controllo amministrativo, fiscale e finanziario della Società e in particolare ha il compito di:

- seguire l'evoluzione dei princìpi e delle normative di carattere contabile, amministrativo e di controllo, provvedendo all'emissione e all'aggiornamento delle procedure contabili della Società;
- definire i calendari delle attività/processi amministrativi verificandone il rispetto;
- contribuire alla definizione delle politiche di bilancio e garantire la predisposizione del bilancio e dei relativi allegati nel rispetto delle normative civilistiche e fiscali;
- mantenere gli opportuni rapporti con il Sindaco Unico e con i consulenti esterni;

assicurare, mediante l'elaborazione dei *report* definiti, il controllo sistematico dei risultati rispetto agli obiettivi pianificati; analizzare le cause di eventuali mancati raggiungimenti, promuovendo azioni correttive.

LA DIREZIONE COMMERCIALE

La direzione commerciale è gestita dal Direttore Commerciale che coordina gli uffici

- Sales
- Marketing Specialist
- Servizio Clienti
- Mercato Privato/ Retail/ PMI (cui fanno capo i responsabili delle singole aree: Area Nord ; Area Toscana ; Area Roma ; Area Caserta)
- Grandi Clienti (cui fanno capo l'area KAM e l'area KAM Agenti)

Questa direzione si occupa della acquisizione e gestione della clientela aziendale.

FUNZIONE OPERAZIONI

La Funzione Operazioni è coordinata dal Responsabile Operazioni cui fanno capo:

- Responsabile Centrale Operativa;
- Responsabile Sviluppo Operativo;
- Back Office;
- i singoli Responsabili di filiale.

FUNZIONE RISORSE UMANE

La Funzione risorse umane ha quali principali compiti quelli di:

- gestire i piani di sviluppo professionale delle risorse umane, definire e aggiornare i piani di rimpiazzo per le posizioni chiave aziendali;
- promuovere e gestire la mobilità delle risorse sia in campo interno che esterno all'azienda;
- sviluppare i piani di comunicazione interna aziendale;
- supportare il CdA nel definire e gestire i cambiamenti organizzativi, nel disegnare l'evoluzione delle strutture e professionalità;
- analizzare, provvedere e contribuire alla gestione degli impatti degli interventi organizzativi ed informatici sulle risorse umane.

FUNZIONE ACQUISTI CORPORATE

Alla Funzione Acquisti è affidato il compito di gestire le modalità e i criteri di scelta dei fornitori di beni e servizi e dei consulenti, garantendo l'ottimizzazione dei relativi costi e un elevato grado di qualità.

DIREZIONE CONTROLLO E RECUPERO CREDITI

A tale Direzione fanno capo gli uffici:

- Controlling;
- Fatturazione (Ufficio contratti);

RECUPERO CREDITI.FUNZIONE IT CORPORATE

Alla Funzione IT è affidato il compito di gestire i sistemi informatici della società, garantendo la protezione della singola postazione di lavoro e delle reti/software aziendali nonché la sicurezza fisica dei sistemi informatici.

DIREZIONE SISTEMI DI SICUREZZA E INNOVAZIONE

Questa Direzione coordina gli uffici:

- Ricerca e Sviluppo;
- Control Room e supporto IT;
- Configurazione Impianti / Assistenza.

FUNZIONE ORGANIZZAZIONE AZIENDALE

Funzione Organizzazione aziendale ha il compito di organizzare ed attuare le linee strategiche societarie in un'ottica di ottimizzazione dei processi operativi ed organizzativi.

DIREZIONE VIGILANZA CORPORATE

La Direzione Vigilanza ha il compito di sovrintendere e gestire l'erogazione dei servizi offerti nel rispetto della normativa vigente, garantendo l'efficienza dei servizi erogati nonché la corretta applicazione dei controlli, espletati a più livelli.

Ai principali servizi della società sono affidate le responsabilità come si seguito elencate.

SERVIZI DI VIGILANZA

- gestire gli uomini e i mezzi dedicati alla erogazione del servizio di vigilanza secondo le indicazioni fornite dal Responsabile;
- provvedere alla corretta gestione dei mezzi e degli equipaggiamenti in dotazione al personale;
- assicurare la erogazione dei servizi di vigilanza, nel pieno rispetto della legislazione vigente in materia di lavoro e di pubblica sicurezza;
- garantire l'addestramento professionale del personale operativo, con particolare riguardo alla sicurezza al mantenimento in efficienza e alla conoscenza nell'uso dei mezzi e degli strumenti in dotazione per l'esecuzione del servizio;
- garantire la corretta gestione dei mezzi di difesa e di intervento in dotazione al personale operativo;
- garantire la corretta efficienza del parco automezzi, delle strutture esterne e assicurare la disponibilità della corretta documentazione richiesta dalla vigente normativa;
- supervisionare l'operato degli operatori di vigilanza;
- adottare per le non conformità di servizio, gli opportuni interventi correttivi secondo quanto stabilito dalle procedure aziendali.

B. STATO DELLE PROCEDURE E OBIETTIVI PERSEGUITI CON L'ADOZIONE DEL MODELLO

L'acquisizione delle Certificazioni di Qualità alla norma UNI EN ISO 14001:2004, UNI EN ISO 45001:2018, SA 8000, UNI PdR 125:2022, UNI EN ISO 9001:2015, ISO 27001:2022, ISO 22301:2019, ISO 39001:2012e alla norma UNI ISO 37001:2016 , 37001 e SA 8000 – Rating Legalità – Iso Parità di genere, testimonia la volontà di Rangers S.r.l. di dotarsi di un Sistema di Gestione della Qualità, nonché delle relative procedure corrispondenti alla norma e atte a uniformare le attività aziendali a *standard* di eccellenza universalmente riconosciuti.

Nel 2023, Rangers, ha inoltre ottenuto dall'Autorità Garante della Concorrenza e del Mercato AGCM il rinnovo del Rating di Legalità ai sensi dell'art. 2, comma 1, del Regolamento adottato dall'AGCM con delibera n. 28361 del 28 luglio 2020, con il punteggio massimo realizzabile.

La Società, inoltre, intende promuovere e consolidare al proprio interno una cultura di trasparenza, integrità e controllo nell'esercizio delle attività aziendali, nella convinzione che l'assoluto rispetto di questi valori rappresenti una premessa indispensabile ai fini del raggiungimento degli obiettivi aziendali di eccellenza.

Nell'ottica di predisporre una ancor più efficiente attività di controllo e di monitoraggio di tutti i processi sensibili, la Società si è dotata di un Modello Organizzativo specificatamente aderente

alle disposizioni del D.lgs. 231/01 quali, in particolare:

- l'introduzione e l'aggiornamento continuo di una serie di procedure operative interne, finalizzate a costituire un valido strumento a presidio delle potenziali aree a rischio reato;
- l'adozione di un Codice Etico;
- l'istituzione delle funzioni Risk Management e Antiriciclaggio (di Gruppo);
- la previsione di un Organismo di Vigilanza e di un sistema sanzionatorio;
- la mappatura dei processi e delle attività aziendali "sensibili" ovvero delle aree operative nel cui ambito potrebbe essere più frequente la possibilità di commissione dei reati di cui al Decreto.

C. SISTEMA DI DELEGHE E PROCURE

La distribuzione dei poteri interni e di rappresentanza verso l'esterno è in sintonia con quanto definito dalle pratiche di legge e da una corretta gestione aziendale. La distribuzione è così caratterizzata dal principio di assegnazione delle responsabilità al personale avente le adeguate competenze.

La distribuzione dei poteri e delle responsabilità assicura un adeguato controllo risultando coerente con la complessità della Società e dei suoi processi operativi grazie anche all'applicazione del principio della separazione dei compiti (c.d. *segregation of duties*), in base al quale nessuno può gestire in autonomia un intero processo.

PRINCIPI GENERALI

Il sistema di deleghe e procure è redatto con chiarezza e adeguatamente presentato ai dirigenti, dipendenti e collaboratori.

Sono identificate con precisione le attribuzioni di responsabilità, le linee di riporto e di gerarchia interna, l'assegnazione di attività e di compiti gestionali e operativi.

L'assetto organizzativo della Società consente di individuare con precisione i soggetti dotati di specifici poteri che possono assumere, in nome e per conto della stessa, obbligazioni verso terzi o che svolgano attività implicanti un contatto diretto con la Pubblica Amministrazione.

Nella predisposizione dell'assetto organizzativo interno, è correttamente definito il sistema delle responsabilità, con particolare attenzione alla separazione delle funzioni, alla descrizione di ruoli aziendali con poteri di rappresentanza e di firma, che possono assumere obbligazioni in nome e per conto della Società e ai relativi tetti di spesa consentiti.

L'assetto organizzativo e il sistema procuratorio sono aggiornati in presenza di variazioni dell'organigramma o dei ruoli/funzioni delegati.

DELEGHE: CRITERI DI ATTRIBUZIONE

Per "**delega**" s'intende quell'atto interno di attribuzione di poteri, compiti e funzioni che specifica il contenuto gestionale delle *job description* e viene riversato nel modello di organizzazione aziendale. Se ineludibile rimane la responsabilità del vertice circa la scelta effettuata (*culpa in eligendo*), i criteri di attribuzione della delega di funzioni sono espressione di parametri mutuati dalla giurisprudenza.

La delega di funzioni non esclude l'obbligo di vigilanza in capo al delegante, in ordine al corretto espletamento da parte del delegato delle funzioni trasferite.

PROCURE: CRITERI DI ATTRIBUZIONE

Per "**procura**" s'intende il negozio giuridico unilaterale con cui l'azienda attribuisce poteri di rappresentanza nei confronti dei terzi. I principi del Decreto Legislativo 231/2001 prevedono un sistema di procure e poteri di firma, atti a garantire una gestione del sistema aziendale efficiente e nel contempo affidabile e trasparente, anche nei confronti dei terzi.

I criteri di assegnazione delle procure sono i seguenti:

- Le procure generali vengono conferite soltanto ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza dell'azienda, coerentemente con il potere di gestione attribuito al titolare attraverso la delega;
- le procure speciali descrivono i poteri di gestione conferiti, l'estensione dei poteri di rappresentanza e i limiti del potere di firma e/o di spesa;
- le procure sono aggiornate tempestivamente in caso di eventi incompatibili con la prosecuzione del mandato (assunzione di nuove responsabilità e poteri, trasferimento ad altri incarichi operativi, dimissioni, licenziamento, revoca,etc.).

MODALITÀ DI ESERCIZIO DI DELEGHE E PROCURE

In relazione alla necessità di rendere efficiente e snello il processo operativo nella fase attuativa, il Consiglio di Amministrazione può conferire poteri specifici per categorie di atti:

- i poteri da esercitarsi con firma singola riguardano quegli atti che rientrano nelle mansioni tipiche del dirigente, il cui esercizio, nei limiti del valore assegnato in procura, costituisce un dovere per il delegato;
- i poteri da esercitarsi con firma abbinata a quella di altro procuratore abilitato a compiere i medesimi atti riguardano le attività così come stabilite dallo Statuto, al quale si rimanda (ad oggi non contemplati)

Firma singola: l'esercizio dei poteri con firma singola potrà avvenire nell'ambito delle materie di competenza del dirigente/procuratore, dopo aver controllato che la pratica sia stata correttamente istruita dalle funzioni competenti.

Firma abbinata: la prima firma sarà apposta dal dirigente/procuratore responsabile dopo che avrà controllato che la pratica sia stata correttamente istruita dalle funzioni competenti (ad oggi non contemplata).

La seconda firma sarà richiesta a procuratore che abbia competenze sufficienti a valutare la corretta istruttoria della pratica e sia in grado di esprimere una valutazione sul merito della stessa.

4. SISTEMA NORMATIVO INTERNO

A. EMANAZIONE DELLA NORMATIVA AZIENDALE

Il Gruppo Battistolli si è dotato di una procedura uniforme per l'emanazione della normativa interna (Procedura aziendale 1.1 "Emanazione e gestione della normativa aziendale") che garantisce:

- la corretta distribuzione dei poteri tra soggetti diversi, sempre definiti o definibili, dotati delle adeguate competenze, che intervengono nelle differenti fasi di attuazione, gestione e autorizzazione delle attività;
- il coordinamento tra le Funzioni aziendali coinvolte;
- idonee iniziative per la diffusione, l'informazione e la comprensione delle regole emanate, in modo tale da garantire l'omogeneità dell'applicazione delle stesse all'interno del Gruppo, nonché la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo.

La regolamentazione del potere normativo interno, evitando la parcellizzazione nell'emanazione delle regole interne, assicura l'idoneità e l'effettività del presente Modello organizzativo.

B. IL CODICE ETICO

In aggiunta ai protocolli di gestione del rischio-reato nell'ambito dei processi sensibili, la Società adotta il Codice Etico del Gruppo Battistolli, approvato dal Consiglio di Amministrazione della *holding* B.M.C. S.p.A. in data 01.06.2018 e da ultimo revisionato in data 20 ottobre 2023, che qui si ritiene integralmente riportato e allegato. Il Codice etico adottato formalizza i valori etici fondamentali ai quali si ispira l'azione aziendale e ai quali i destinatari dello stesso si devono attenere nello svolgimento dei compiti e delle funzioni loro affidate.

Le regole di condotta e il Codice Etico costituiscono parte integrante del presente Modello e della normativa aziendale. Il Modello presuppone il rispetto di quanto previsto nel Codice Etico, formando con esso un *corpus* di norme interne finalizzate alla diffusione di una cultura improntata all'etica e alla trasparenza aziendale.

In particolare:

- il Codice Etico rappresenta uno strumento da adottarsi in via autonoma e suscettibile di applicazione sul piano generale che esprime i principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti gli Organi sociali, i dipendenti e tutti i collaboratori esterni;
- il Modello risponde, invece, a specifiche prescrizioni contenute nel D.lgs. 231/01, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi apparentemente a vantaggio dell'azienda, possono comportare una responsabilità amministrativa da reato in base alle disposizioni del decreto medesimo). Il Modello detta le

regole e prevede le procedure che devono essere rispettate al fine di costituire l'esimente per la Società ai fini della responsabilità di cui al D.lgs. 231/01.

Il compito di vigilare sulla corretta e costante applicazione aziendale del Codice Etico viene affidato all'Organismo di Vigilanza. Le segnalazioni di violazioni o sospette violazioni al Codice Etico che si sovrappongonoopresentinoprofilidiconnessioneconireatipresuppostodelD.lgs.231/01, sono trasmesse per competenza all'Organismo di Vigilanza. Qualora l'OdV, nell'ambito delle proprie attività, abbia notizia di violazioni o sospette violazioni al Codice Etico che non competano alle sue funzioni, trasmette la notizia al Consiglio di Amministrazione.

Il Codice Etico, in tutte le sue future riformulazioni, è suscettibile di modifiche e/o integrazioni in ragione dell'evoluzione delle norme di legge e delle mutate esigenze aziendali.

D. C. ORGANISMO DI VIGILANZA

Rangers S.r.l. ha costituito il proprio Organismo di Vigilanza (di seguito anche "OdV"), quale organismo indipendente, che assume i compiti previsti dalla normativa (art. 6, comma 1, lett. b, del Decreto).

In ossequio al dettato di legge e in conformità alle linee-guida emanate da Confindustria, l'OdV è chiamato a verificare l'adeguatezza e l'effettività del Modello Organizzativo e del Codice Etico, curarne l'aggiornamento, garantire la conservazione dei requisiti di solidità, funzionalità ed efficacia del Modello, vigilare sulla relativa applicazione, nonché assicurare l'effettività dei flussi di informazioni tra gli Organi direttivi, le Funzioni aziendali e l'OdV stesso e segnalare le violazioni eventualmente accertate.

Per la disciplina dettagliata del proprio funzionamento l'OdV adotta un regolamento interno, comunicato al Consiglio di Amministrazione.

NOMINA E DURATA

Il Consiglio di Amministrazione nomina l'OdV, garantendo i necessari profili di indipendenza, autonomia, professionalità, onorabilità e continuità di azione, ne valuta periodicamente l'adeguatezza e, quando necessario, provvede alla sostituzione dei membri che dovessero cessare dal loro incarico.

La nomina dei membri dell'OdV è formalmente accettata dai membri, attraverso la sottoscrizione di una lettera di incarico predisposta dalla Società, ed è resa nota dalla Direzione aziendale e a tutto il personale della Società.

L'Organismo di Vigilanza resta in carica per il numero di esercizi sociali stabilito dal Consiglio di Amministrazione all'atto di nomina e comunque (ovvero in assenza di sua determinazione all'atto di nomina) non oltre tre esercizi. I suoi membri sono rieleggibili, salva l'insorgenza di una causa di revoca o la sopravvenuta carenza dei requisiti di cui dopo.

REQUISITI DI PROFESSIONALITÀ

L'OdV di Rangers S.r.l. è un organo collegiale composto da tre membri esterni. In linea generale i

profili dei componenti garantiscono competenze relative a:

- sistemi di controllo interno, tecniche di analisi e valutazione dei rischi, e misure per il loro contenimento;
- organizzazione aziendale;
- diritto penale d'impresa;

I membri dell'OdV sono scelti dal Consiglio di Amministrazione tra figure professionali che garantiscono autonomia, indipendenza e continuità d'azione.

REQUISITI, RECESSO E CAUSE DI REVOCA

Ai fini della effettiva ed efficace attività di controllo sull'attuazione e aggiornamento del Modello, l'Organismo di Vigilanza deve possedere specifici requisiti individuati dal legislatore e poi meglio dettagliati dalla giurisprudenza, dalla dottrina e dalla prassi.

Si tratta, per lo più, di caratteristiche in grado di consentire all'azione di controllo l'effettività da cui il Decreto fa derivare anche l'efficacia esimente del Modello.

Pertanto, il CdA nomina un OdV che sia in grado di svolgere i compiti a esso affidati e che possiede i seguenti requisiti:

- indipendenza, vale a dire l'esigenza che non vi siano, neanche potenzialmente, conflitti di interesse con la Società o legami con i vertici della stessa o comunque con il gruppo di comando;
- autonomia, vale a dire autonomi poteri di iniziativa e di controllo; all'OdV deve dunque essere riconosciuta una autonomia decisionale nello svolgimento della propria attività, che si esprime nella necessità di libertà di autodeterminazione e di azione con pieno esercizio della discrezionalità tecnica nell'espletamento delle funzioni, e garantiti poteri adeguati allo svolgimento dei propri compiti;
- professionalità, vale a dire competenze e abilità ispettive e consulenziali, oltre che tecnico-professionali. Per poter ricoprire il ruolo di membro dell'OdV è necessario avere professionalità che consentano di svolgere adeguatamente ed efficacemente il proprio ruolo ed essere in possesso di «*tecniche specifiche, idonee a garantire l'efficacia dei poteri di controllo e del potere propositivo ad esso demandato*» (Trib. Napoli, ordinanza 26 giugno 2007). È quindi necessaria una doppia professionalità: la prima in possesso di chi ha dimestichezza con tecniche specialistiche proprie di chi svolge attività *lato sensu* ispettiva o comunque di analisi dei sistemi di controllo; la seconda, invece, di tipo giuridico e, più in particolare, penalistico;
- onorabilità, intesa come assenza di cause di ineleggibilità, previste per i soggetti che svolgono funzioni di amministrazione, direzione e controllo;
- e continuità aziendale, in quanto l'attività di monitoraggio e vigilanza deve essere esercitata in maniera costante e continua. L'OdV deve assicurare un funzionamento

costante nel tempo e in continua interazione con gli organismi amministrativi e di controllo delle società. È necessaria, pertanto, la creazione di una struttura dedicata a tempo pieno ed esclusivamente all'attività di vigilanza sul modello stesso.

I componenti dell'OdV, dunque, al momento della nomina e per tutta la durata del loro incarico, non devono:

a) rivestire incarichi esecutivi o delegati nel Consiglio di Amministrazione di Rangers S.r.l..;

b) avere rapporti con o far parte del nucleo familiare degli Amministratori, intendendosi per nucleo familiare quello costituito dal coniuge e dai parenti e affini entro il quarto grado;

c) essere stati sottoposti a misure di prevenzione previste dall'art. 10, comma 2, L. 31 maggio 1965, n.575, come sostituito dall'art. 3 L. 19 marzo 1990, n. 55 e successive disposizioni;

d) essere stati condannati, con sentenza anche se emessa *ex* art. 444 e ss. c.p.p., per uno qualunque dei reati richiamati dal D.lgs. 231/01, salvi gli effetti della riabilitazione.

Al fine dell'accertamento dei requisiti, i candidati devono presentare in tempo utile al Consiglio di Amministrazione un *curriculum vitae*. I componenti dell'OdV sono tenuti a comunicare immediatamente al Consiglio di Amministrazione l'insorgere di una delle condizioni che comporti il venir meno dei requisiti di eleggibilità e onorabilità di cui ai punti precedenti.

L'Organismo di Vigilanza termina il proprio incarico per naturale scadenza del mandato, decadenza o revoca per giusta causa da parte dell'ente ovvero per rinuncia da parte di uno o di tutti i suoi componenti.

Cause di cessazione dell'incarico dell'Organismo di Vigilanza
1. scadenza dell'incarico;
2. decadenza;
3. revoca per giusta causa da parte dell'ente;
4. rinuncia.

Tali situazioni non sono regolate dal Decreto, si applica pertanto la disciplina espressamente prevista per fattispecie sovrapponibili a queste. In ogni caso, la revoca dell'Organismo di Vigilanza compete al Consiglio di Amministrazione.

Cause tassative di revoca dell'OdV sono le seguenti:

- la perdita dei requisiti di eleggibilità (indipendenza, professionalità, autonomia, onorabilità);
- inadempimento agli obblighi di vigilanza e di controllo;
- accertamento da parte dell'amministratore di negligenza, imperizia o colpa grave nello svolgimento dei compiti assegnati nonché, nei casi più gravi, della commissione di reati;

- Prolungata inattività;
- Violazione degli obblighi di riservatezza sulle informazioni acquisite nell'ambito dello svolgimento delle attività di vigilanza;
- mancata segnalazione di situazioni critiche al Consiglio di Amministrazione;
- sentenza di condanna, anche non definitiva, a carico dei componenti dell'OdV per aver personalmente commesso uno dei reati presupposto di cui al Decreto
- sentenza di condanna passata in giudicato, a carico dei componenti dell'OdV, a una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Ciascun componente dell'Organismo di Vigilanza può recedere in ogni momento dall'incarico, mediante preavviso di almeno due mesi, attraverso comunicazione scritta e motivata al Consiglio di Amministrazione.

In caso di recesso o decadenza di uno dei componenti dell'OdV, il Consiglio di Amministrazione provvede tempestivamente alla sua sostituzione.

AUTONOMIA FINANZIARIA

Perché sia assicurata la piena autonomia e possa esercitare pienamente le proprie funzioni, l'OdV dispone di adeguate risorse finanziarie, sulla base di un *budget* annuale di spesa approvato dal Consiglio di Amministrazione della Società su proposta dell'OdV stesso. L'impiego delle risorse del *budget* è oggetto di rendicontazione annuale da parte dell'OdV.

In presenza di situazioni eccezionali o urgenti l'OdV può chiedere al Presidente del Consiglio di Amministrazione, salva successiva ratifica del Consiglio di Amministrazione, risorse eccedenti la propria autonomia di spesa.

Nell'esercizio delle sue funzioni, l'OdV può avvalersi della collaborazione di esperti, a cui sarà conferito specifico incarico da parte dell'Organismo stesso, nell'ambito della sua autonomia e nei limiti del *budget* assegnato, salvo comunicazione al Consiglio di Amministrazione.

Il compenso dei membri dell'Organismo di Vigilanza è fissato dal CdA.

AUTONOMIA FUNZIONALE

L'OdV dispone di autonomi poteri di iniziativa e di controllo, tali da consentire l'efficace esercizio delle sue funzioni.

Decide le proprie azioni e iniziative senza richiedere autorizzazioni e senza informare preventivamente il Consiglio di Amministrazione o la direzione aziendale.

Ha accesso a tutte le informazioni e alla documentazione della Società necessarie per lo svolgimento della propria attività di vigilanza.

Può convocare il personale della Società e i suoi amministratori per chiedere informazioni,

chiarimenti o l'esibizione di documenti in merito alle attività sensibili previste.

All'OdV non competono, né possono essere attribuiti, neppure in via sostitutiva, poteri di intervento gestionale e decisionale relativi allo svolgimento delle attività di Rangers S.r.l..

L'OdV svolge le sue funzioni curando e favorendo una razionale ed efficiente cooperazione con le altre funzioni di controllo della Società.

COMPITI E ATTIVITÀ

L'OdV si atteggia, sul piano funzionale, come uno strumento di controllo, pervasivo, sull'effettività e l'adeguatezza del modello di prevenzione del rischio-reato. Tale obbiettivo viene perseguito, sinergicamente, tramite l'espletamento di attività informative e di controllo, a cui si affiancano poteri propositivi e di accertamento disciplinare. A tal fine, l'Organismo di Vigilanza di Rangers S.r.l. è dotato di tutti i poteri necessari per assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello organizzativo adottato, secondo quanto stabilito dall'art. 6 del D.lgs. n. 231/2001.

In particolare, compete all'OdV vigilare:

- sull'effettività del Modello, e quindi sulla coerenza tra i comportamenti concreti e quanto il Modello istituito prevede. In tale ambito, l'OdV deve:
    - attivare le procedure di controllo e verificare che le stesse siano adeguate e rispondenti alle esigenze di osservanza di quanto prescritto dal D.lgs. 231/2001;
    - disporre periodicamente verifiche su determinate operazioni, processi o atti specifici posti in essere nell'ambito delle aree di attività "sensibili";
    - coordinarsi con le altre funzioni aziendali per il migliore monitoraggio delle attività "sensibili". A tal fine, l'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale che ritiene rilevante; deve essere tenuto costantemente informato dagli Organi Sociali e dai responsabili delle unità operative sugli aspetti dell'attività aziendale che possono esporre la Società al rischio di commissione dei reati;
    - effettuare verifiche relative al grado di conoscenza acquisito dal personale dipendente rispetto alle ipotesi di reato previste dal D.lgs. 231/2001 e al Modello adottato, anche tramite interviste a campione;
    - attivare indagini interne, anche con l'eventuale collaborazione delle strutture aziendali, per la raccolta, l'elaborazione e la conservazione delle informazioni rilevanti in ordine al rispetto del Modello e per l'accertamento di presunte violazioni delle prescrizioni del Modello stesso;
        - valutare in merito all'adeguatezza del Modello, ossia alla sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;

- curare il necessario aggiornamento del Modello, in relazione a mutate condizioni aziendali e/o a nuove normative e comunque nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni e adeguamenti;
- ricevere e gestire le segnalazioni di illeciti da parte dei dipendenti;

➢ sull'attività di diffusione del Modello all'interno della Società e di informazione nei confronti dei soggetti esterni (fornitori, consulenti, collaboratori). In particolare, l'OdV deve:

- promuovere idonee iniziative per la diffusione, l'informazione e la comprensione del Modello;
- predisporre la documentazione organizzativa interna necessaria al funzionamento del Modello stesso, contenente istruzioni, chiarimenti o aggiornamenti;

➢ sull'attività di formazione sui contenuti del Decreto e del Modello nei confronti di tutto il personale dipendente e a contratto libero professionale della Società. A tale scopo, esso deve:

- definire, insieme al *management*, (i) i programmi di formazione per il personale dipendente; (ii) il contenuto delle comunicazioni periodiche agli Organi Sociali, al personale dipendente e ai collaboratori esterni, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al Decreto;
- verificare la completa attuazione dei piani di formazione sul Decreto e sul Modello.

In aggiunta ai compiti previsti dall'art. 6, lett. b), D.lgs. 231/2001 come sopra elencati, con l'entrata in vigore d.lgs. 231/2007 – in attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo – e fino all'introduzione D.lgs. 90/2017, che ha dato attuazione alla IV direttiva antiriciclaggio, erano previsti una serie di ulteriori obblighi anche con riferimento all'Organismo di Vigilanza, tanto che nel d.lgs. 231/2007, all'art. 52, comma 1, rubricato «Organi di controllo», oltre al collegio sindacale, al consiglio di sorveglianza, al comitato di controllo di gestione e a tutti i soggetti incaricati del controllo di gestione comunque denominati veniva citato anche «l'Organismo di Vigilanza di cui all'art. 6, comma 1, lett. b) d.lgs. 231/2001» tra i soggetti destinatari degli obblighi di comunicazione previsti dal d.lgs. 231/2007, individuati nella stessa disposizione.
Con l'entrata in vigore del D.lgs 90 del 2017 è venuto a cadere ogni riferimento all'Organismo di Vigilanza nell'ambito della disciplina antiriciclaggio: le precedenti versioni degli artt. 52 e 55, d.lgs. 231/2007 sono state integralmente riformulate dalla modifica normativa. In primo luogo, l'art. 46, D.lgs. 90/2017, che ha sostituito l'art. 52, d.lgs. 231/2007, non prevede più tra i soggetti obbligati alle comunicazioni l'Organismo di Vigilanza. Infatti, gli organi di controllo tenuti a tali comunicazioni,

secondo la previsione del nuovo art. 46, d.lgs. 231/2007 sono «i componenti del Collegio Sindacale, del consiglio di sorveglianza e del comitato per il controllo sulla gestione presso i soggetti obbligati». La riforma introdotta dal d.lgs. 90/2017 conferma, dunque, la tesi prevalente in giurisprudenza della natura dell'Organismo di Vigilanza quale soggetto a rilevanza esclusivamente interna, deputato a garantire solo il funzionamento e il rispetto delle procedure organizzative previste nei Modelli di organizzazione, gestione e controllo, senza attribuirgli alcuna posizione di garanzia con riferimento all'impedimento di delitti da parte degli organi apicali dell'ente.
Ciò non comporta ovviamente che i componenti dell'Organismo di Vigilanza, in tema di riciclaggio e autoriciclaggio, non dovranno più procedere alle attività di monitoraggio dei presidi di controllo adottati dalla società in tema di prevenzione dei reati di riciclaggio e autoriciclaggio previsti dall'art. 25 octies, d.lgs. 231/2001. La presenza di procedure e protocolli atti a impedire la commissione dei reati sopra menzionati, infatti, resta, uno dei più importanti profili da considerare affinché un Modello di organizzazione, gestione e controllo possa essere ritenuto esimente dalla responsabilità da reato nel caso uno dei suoi soggetti apicali o sottoposti commetta un illecito ai sensi degli artt. 648 bis e 648 ter.1 c.p.

Alla luce di quanto sopra esposto, si può concludere che i compiti dell'Organismo di Vigilanza hanno rilevanza nell'interesse esclusivo dell'ente per cui opera al fine di evitare che questo possa subire le conseguenze di condotte illecite tenute dai soggetti previsti all'art. 5, lett. a), del Decreto stesso, mentre non hanno alcuna rilevanza esterna verso soggetti diversi dalla persona giuridica nel cui ambito opera, con la conseguenza che il mancato corretto svolgimento dei compiti assegnatigli non può in alcun modo integrare la violazione di un precetto penale.
Infine, è chiaramente compito dell'OdV proporre procedimenti sanzionatori ove si riscontrino situazioni di violazione del Modello o del Codice Etico.

OBBLIGHI INFORMATIVI DELL'ORGANISMO DIVIGILANZA

L'OdV riferisce esclusivamente al Consiglio di Amministrazione della Società.

Nei casi di urgenza, può riferire direttamente al Presidente del CdA della Società, salvo informare successivamente l'intero Consiglio di Amministrazione.

Circa il flusso informativo in direzione del vertice aziendale, l'OdV è tenuto:

- a convogliare, con periodica regolarità, *report* sull'attività svolta, contenente:
    - la sintesi delle attività svolte nel semestre;
    - eventuali mutamenti del quadro normativo o dell'assetto organizzativo che richiedono un aggiornamento del Modello;
    - un rendiconto delle spese sostenute;
- a trasmettere, con tempestività, tutte le informazioni riguardanti eventuali violazioni del Modello;
- segnalare la necessità di un adeguamento del Modello, in presenza di un *deficit* di effettività o di modificazioni del tessuto organizzativo aziendale.

In caso di violazione accertata del Modello, l'OdV riferisce con immediatezza al Presidente di Rangers S.r.l., che riferisce al Consiglio di Amministrazione nella prima seduta utile.

Qualora dalle violazioni del Modello possano derivare conseguenze dannose per la Società, l'OdV informa anche il Sindaco Unico.

Il Consiglio di Amministrazione ha la facoltà di convocare in qualsiasi momento l'OdV il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione del CdA per motivi urgenti.

OBBLIGHI INFORMATIVI VERSO L'ORGANISMO DIVIGILANZA

Sul versante informativo, giuoca un ruolo decisivo il piano delle informazioni e delle comunicazioni verso l'OdV. L'effettività dei flussi informativi dipende dalla chiara individuazione del canale di comunicazione, cioè dall'esistenza di un responsabile del processo a rischio-reato, che funga da interfaccia informativa dell'OdV.

Le segnalazioni verso l'OdV possono riguardare tutte le violazioni del Modello, anche solo presunte, e fatti, ordinari e straordinari, rilevanti ai fini dell'attuazione e dell'efficacia dello stesso.

Tutto il personale di Rangers S.r.l.e i membri degli organi direttivi sono tenuti a segnalare all'OdV:

- fatti che integrano o possono ragionevolmente integrare un reato;
- violazioni o sospetti di violazioni delle norme comportamentali richiamate dal Codice Etico;
- deroghe, violazioni o sospetti di violazioni dei principi generali di organizzazione e gestione richiamati nel Modello;
- deroghe, violazioni o sospetti di violazioni delle procedure aziendali che disciplinano le attività a rischio di reato,

di cui sono a diretta conoscenza o di cui sono venuti a conoscenza tramite comunicazione altrui.

Devono in ogni caso essere obbligatoriamente trasmesse all'OdV le seguenti informazioni:

- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati presupposto del D.lgs. 231/2001;
- le richieste di assistenza legale inoltrate dai dirigenti e dipendenti in caso di avvio di procedimento giudiziario per i reati di cui al D.lgs.231/2001;
- i rapporti eventualmente preparati dai responsabili delle funzioni aziendali e/o unità operative nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.lgs.231/2001;
- le notizie relative ai procedimenti disciplinari originati dalla violazione delle prescrizioni contenute nei Protocolli predisposti *ex* D.lgs. 231/01 o per violazione del Codice Etico e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero ai

provvedimenti di archiviazione di tali procedimenti comprendenti le relative motivazioni;

- le segnalazioni di illeciti da parte dei dipendenti;
- i verbali di accertamento, i provvedimenti di contestazione.

Tutte le segnalazioni, comprese quelle che hanno ad oggetto l'evidenza o il sospetto di violazione del Modello, dei principi generali e dei principi sanciti nel Codice Etico, devono pervenire per iscritto.

Le comunicazioni all'Organismo di Vigilanza devono essere effettuate tramite l'indirizzo e-mail odv.rangers@battistolli.it alla casella di posta elettronica (protetta da *password* e conforme ai protocolli di tutela dei dati adottati da PSD) contrassegnata dal presente indirizzo accedono, con credenziali di autenticazione individuali, i soli membri dell'OdV.

Le modalità di segnalazione sono rese note a tutto il personale della Società e a tutti i membri degli Organi sociali attraverso i mezzi ritenuti più opportuni (es. *intranet*, bacheche, comunicazioni interne).

Compito dell'Organismo di Vigilanza è garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando anche la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede; il venir meno a tale obbligo rappresenta una grave violazione del Modello.

Ricevuta la segnalazione, l'Organismo di Vigilanza, valutata la non pretestuosità della segnalazione, deve immediatamente dare corso ai necessari accertamenti, garantendo la riservatezza del soggetto nei cui confronti procede.

Valutata la rilevanza e la fondatezza della segnalazione e della violazione, l'OdV informa immediatamente il titolare del potere disciplinare.

Tra i protocolli posti a presidio delle aree/processi a rischio, devono essere specificamente formalizzati i "flussi informativi" (attraverso la redazione di *report*) relativi a informazioni/dati/notizie (riguardanti l'andamento di attività sensibili) identificati dall'OdV e da questo richiesti alle singole funzioni aziendali coinvolte, nei tempi e nei modi che saranno definiti dall'OdV.

5. SEGNALAZIONI DI ILLECITI DA PARTE DEI DIPENDENTI

Nel rispetto delle disposizioni di legge per la tutela del dipendente che segnala reati o irregolarità di cui sia venuto a conoscenza nell'ambito del rapporto di lavoro, Rangers S.r.l. si dota di appositi canali attraverso i quali effettuare la segnalazione di illeciti da parte del personale, che siano idonei a garantire la riservatezza dell'identità del segnalante.

La Società assicura, altresì, la tutela del segnalante da possibili atti ritorsivi, diretti o indiretti, ricollegabili alla segnalazione. È previsto un sistema di sanzioni da comminare nel caso in cui il segnalante, in mala fede, abbia avanzato una segnalazione rivelatasi falsa o infondata.

DEFINIZIONI

Contesto lavorativo: in materia di whistleblowing, per contesto lavorativo si intendono le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'art.3, commi 3 o 4 del d.lgs. n. 24/2023, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'Autorità giudiziaria o contabile.

Destinatario della segnalazione: soggetto o organo della Società avente il compito di ricevere, analizzare e verificare le segnalazioni. Per la Società le segnalazioni dovranno pervenire Ufficio Segnalazioni Illeciti Whistleblowing, quale Ufficio preposto alla gestione delle segnalazioni, la cui analisi, spetterà, per competenza alle diverse Figure di controllo presenti in azienda.

Divulgazione pubblica: rendere di pubblico dominio informazioni sulle violazioni – di cui alla disciplina in materia di *whistleblowing* – tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

Facilitatore: in materia di *whistleblowing*, è definita tale la persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.

Persona coinvolta: in materia di *whistleblowing*, si definisce tale la persona fisica o giuridica menzionata nella segnalazione interna o estera ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.

Ritorsioni: in materia di *whistleblowing*, si definisce tale qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto;

Segnalante (o *Whistleblower*): in materia di *whistleblowing* si definisce tale la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;

Segnalazione: comunicazione del segnalante avente a oggetto il ragionevole e legittimo sospetto o la consapevolezza di comportamenti illegittimi o irregolarità, commessi da dipendenti o rappresentanti dell'azienda, che possano recare un danno, anche solo di immagine, alla società, nonché a terzi. La segnalazione interna è la comunicazione delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna;vla segnalazione esterna è la comunicazione

delle informazioni sulle violazioni, presentata tramite il canale istituito dall'Autorità Nazionale Anticorruzione (ANAC).

PRINCIPI GENERALI

- **Indipendenza e professionalità del destinatario della segnalazione**: il destinatario della segnalazione svolge le proprie attività assicurando il mantenimento delle necessarie condizioni di indipendenza e la dovuta obiettività, competenza e diligenza professionali.
- **Garanzia di riservatezza**: le procedure attraverso le quali si effettua la segnalazione devono garantire la riservatezza del segnalante, a eccezione dei casi in cui sia la normativa in vigore a richiedere che venga esclusa. Tutte le persone che ricevano una Segnalazione e/o che siano coinvolte, a qualsivoglia titolo, nell'istruzione e trattazione della stessa, sono tenute a garantire la massima riservatezza sui soggetti e sui fatti segnalati, utilizzando, a tal fine, criteri e modalità di comunicazione idonei a tutelare l'identità e l'onorabilità delle persone menzionate nelle segnalazioni, nonché l'anonimato dei segnalanti, affinché chi effettua la segnalazione non sia soggetto ad alcuna forma di ritorsione, evitando in ogni caso la comunicazione dei dati acquisiti a soggetti estranei al processo di istruzione e trattazione delle segnalazioni disciplinato nel presente strumento.
- **Divieto di ritorsioni**: è nulla qualsiasi forma di ritorsione o azione discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. In particolare, le ritorsioni di cui può essere vittima il segnalante possono consistere, ad esempio, nel:
    - licenziamento;
    - demansionamento;
    - trasferimento ingiustificato;
    - *mobbing*;
    - molestie sul luogo di lavoro o qualsiasi altro tipo di comportamento che determini condizioni di lavoro intollerabili.

La tutela contro gli atti di ritorsione è estesa a tutti i soggetti collegati all'organizzazione e/o alla persona del segnalante quali:

- lavoratori autonomi, titolari di rapporti di collaborazione, liberi professionisti e consulenti;
- volontari e tirocinanti, retribuiti e non retribuiti;
- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto;
- facilitatori (le persone che assistono il segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata);
- persone appartenenti al medesimo contesto lavorativo del segnalante a lui legate da uno stabile legame affettivo o di parentela;
- colleghi di lavoro del segnalante a lui legati da un rapporto abituale e corrente;

- enti di proprietà del segnalante o per i quali le persone tutelate lavorano, nonché gli enti che operano nel medesimo contesto lavorativo delle persone di cui sopra.

Simili misure di tutela trovano applicazione solo nei confronti del segnalante in buona fede, di colui il quale abbia effettuato una segnalazione concernente una irregolarità o un illecito ritenendo altamente probabile, in base alle proprie conoscenze, che si sia verificato.

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

OGGETTO E CAMPO DI APPLICAZIONE

Le segnalazioni possono avere a oggetto sia condotte illecite rilevanti per il D.lgs. 231/2001 sia violazioni del Modello e del Codice Etico. Ai sensi del D.Lgs. 24/2023 del 10.03.2023 l'oggetto delle segnalazioni è stato esteso anche agli illeciti amministrativi, contabili, civili o penali che ledono l'interesse pubblico o l'integrità dell'ente e agli atti e omissioni che ledono gli interessi finanziari della Unione Europea a/o riguardanti il mercato finanziario interno. Le segnalazioni, infine, possono avere ad oggetto anche condotte volte ad occultare le violazioni di cui sopra.

Le segnalazioni riguardanti le violazioni, potenziali od effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo rimangono specificamente disciplinate e previste, in ottemperanza alle disposizioni di cui al D. Lgs. 21 novembre 2007 e ss.mm.ii. (c.d. Normativa Antiriciclaggio), con apposito canale dedicato, previsto dal Regolamento Antiriciclaggio cui si rinvia: https://rangerswhistleblowing.battistolli.it/

Non è richiesto che il segnalante sia certo dell'effettivo avvenimento dei fatti denunciati e dell'autore degli stessi, ma è sufficiente che, in base alle proprie conoscenze, ritenga altamente probabile che il fatto si sia verificato. È opportuno che le segnalazioni siano il più possibile circostanziate e offrano il maggior numero di elementi utili a effettuare ricerche.

Non sono, invece, meritevoli di tutela le segnalazioni fondate su meri sospetti o voci.

PROCEDURA DI SEGNALAZIONE

La società ha adottato una specifica procedura di segnalazione (Policy aziendale – whistleblowing 8.1), cui si rinvia per i dettagli operativi.

La procedura di segnalazione si snoda in diversi passaggi che devono essere posti in essere dal Segnalante nell'inviare la Segnalazione e dal Soggetto che riceve la segnalazione nello svolgimento dell'istruttoria.

Il canale è affidato ad apposito Ufficio Segnalazioni Illeciti Whistleblowing, interno all'Azienda, con specifica competenza per la gestione delle segnalazioni.

Il canale di segnalazione adottato dalla società è disponibile al seguente link: https://rangerswhistleblowing.battistolli.it/

Nello specifico, il canale di segnalazione adottato prevede differenti "contesti di segnalazione" in virtù dei sistemi di *compliance* adottati dalla Società. In particolare:

- Whistleblowing Antiriciclaggio – relativo alla specifica segnalazione di violazioni, potenziali od effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (per le Società del Gruppo soggette alla normativa Antiriciclaggio – come da previsioni del Regolamento Antiriciclaggio sopra richiamato).
- Whistleblowing 231 – relativo alla specifica segnalazione di violazioni, compiute o tentate, del Codice Etico, del Modello di Organizzazione e dei relativi Protocolli di cui la Società si è dotata.
- Whistleblowing Anticorruzione – relativo alla specifica segnalazione di violazioni, potenziali od effettive, delle disposizioni dettate in funzione di prevenzione della corruzione
- Whistleblowing SA 8000 – relativo alle specifiche segnalazioni di violazioni, potenziali od effettive, delle disposizioni dettate dalla procedura SA 8000

La Segnalazione può comunque essere inviata mediante un canale aperto e coinvolgere ogni ipotesi di illecito amministrativo, contabile, civile o penale che leda l'integrità della Società coinvolta, come pure le condotte volte ad occultare le violazioni di cui sopra. La segnalazione è gestita tramite apposito/a Applicativo/piattaforma informatica, ma può essere anche effettuata mediante canale telefonico, o incontro diretto, a richiesta del Segnalante.

INVIO DELLE SEGNALAZIONI

I lavoratori subordinati o autonomi, i collaboratori che svolgono la propria attività lavorativa presso la Società o presso soggetti che forniscono beni o servizi o che realizzano opere in favore di terzi, i liberi professionisti e i consulenti che prestano la propria attività presso la Società, i volontari e i tirocinanti, (retribuiti e non retribuiti) che prestano la propria attività presso la Società, gli azionisti, i soci e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso l'Ente, inviano all'Ufficio Segnalazioni Illeciti Whistleblowing le segnalazioni secondo le modalità di seguito esposte, non appena vengano a conoscenza degli eventi che le hanno generate.

È previsto un apposito canale di segnalazione attraverso il quale, nel rispetto della *privacy* e dei diritti individuali, tutti coloro i quali vengono a conoscenza di eventuali casi di illeciti possono riferire liberamente e in maniera riservata. L'accesso alle informazioni caricate sulla piattaforma dedicata è consentito, tramite credenziali di autenticazione univoche, ai soli membri incaricati della gestione della segnalazione in relazione allo specifico contesto.

Qualora un dipendente dovesse ricevere, al di fuori dei canali previsti, una segnalazione da altri soggetti (es. dipendenti/terzi), la trasmette, con immediatezza e in via esclusiva, sempre secondo le modalità di seguito esposte, completa di tutta la eventuale documentazione di supporto pervenuta,

non trattenendone copia e astenendosi dall'intraprendere alcuna iniziativa autonoma di analisi e/o approfondimento. La mancata comunicazione di una segnalazione ricevuta può costituire una violazione delle disposizioni del modello organizzativo adottato dalla Società (oltre che del Codice Etico), con l'applicazione in caso di accertata malafede di tali condotte, delle conseguenti sanzioni disciplinari.

La trasmissione della segnalazione, da attuarsi mediante gli appositi canali sopra indicati, prevede:

- il rilascio al segnalante un avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione;
- l'informativa al segnalante della possibilità di essere ricontattato per acquisire eventuali elementi utili alla fase istruttoria, nonché della possibilità di inviare ulteriori informazioni o elementi di cui verrà a conoscenza, ai fini di integrare o aggiornare i fatti oggetto della segnalazione iniziale;
- l'attivazione di un'istruttoria interna;
- la trasmissione di un riscontro entro tre mesi dalla data dell'avviso di ricevimento della segnalazione o, in mancanza, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

A seguito dell'invio della segnalazione, la piattaforma dedicata mostrerà un "codice segnalazione" che consente di monitorare lo stato di avanzamento della segnalazione, di integrarla e di scambiare messaggi con il destinatario.

Il segnalante può procedere alla segnalazione esterna se, al momento della presentazione, ricorre una delle seguenti condizioni;

- non è prevista, nell'ambito del contesto lavorativo del segnalante, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dal decreto;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

La Società garantisce che nessuno in ambito lavorativo possa subire ritorsioni, illeciti, condizionamenti e discriminazioni di qualunque tipo per aver segnalato la violazione dei contenuti del Modello.

ISTRUTTORIA

A seguito della segnalazione di illecito, seguono opportune verifiche e, nel caso, adeguate misure sanzionatorie.

L''Ufficio Segnalazioni Illeciti Whistleblowing deve effettuare un primo *screening* di ammissibilità della segnalazione. In tale attività dovrà valutare:

- se la segnalazione ha lo scopo di sottoporre all'attenzione della Società un comportamento che possa minare alla integrità della stessa, o configura una mera lamentela personale;
- quanto grave e urgente è il rischio per la Società o per i terzi;
- se l'oggetto della segnalazione è già stato valutato in passato;
- se la segnalazione contiene sufficienti elementi per poter essere verificata.

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

TUTELA DEL SEGNALANTE E OBBLIGHI DI RISERVATEZZA

A tutela del segnalante la Società si impegna al rispetto dei seguenti obblighi:

- le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse;
- l'identità del segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il suo consenso espresso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati (titolare e responsabile del trattamento dei dati, ai sensi del Regolamento (UE) 2016/679 e codice in materia di protezione dei dati personali ex D.Lgs. n. 196/2003);
- nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p.;
- nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità; è dato comunque avviso alla persona segnalante delle ragioni della rivelazione dei dati riservati;

- è tutelata altresì l'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore del segnalante;
- beneficia della protezione prevista dal decreto anche il segnalante che effettua una divulgazione pubblica, sui mezzi di informazione, se ricorre una delle condizioni indicate per procedere alla segnalazione esterna;
- la tutela dalle ritorsioni è prevista anche per le segnalazioni o denunce all'autorità giudiziaria o contabile o divulgazioni pubbliche anonime, se la persona segnalante è stata successivamente identificata e ha subìto ritorsioni;
- la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti;
- le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza.

Le tutele sopra indicate non sono garantite al segnalante quando è accertata, anche con sentenza di primo grado, la responsabilità penale dello stesso per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave. In questi casi al segnalante o denunciante è irrogata una sanzione disciplinare.

SANZIONI E PROVVEDIMENTI CONSEQUENZIALI

La Società sanzionerà ogni comportamento illecito, ascrivibile al personale e ai collaboratori della Società, che dovesse emergere a seguito di attività di verifica successiva alla segnalazione.

In particolare, nel caso in cui, all'esito della fase istruttoria, dovessero emergere segnalazioni in mala fede, l'Ufficio Segnalazioni attiverà un procedimento disciplinare nei confronti del segnalante.

La Società adotterà adeguati provvedimenti disciplinari, secondo quanto disposto dal Modello di organizzazione, gestione e controllo e dal contratto collettivo di lavoro o dalle altre norme nazionali applicabili, nei confronti di coloro che:

a) a seguito di attività di verifica successiva a una segnalazione, risultino responsabili della violazione delle disposizioni contenute nel D.lgs. 231/2001, nonché di quanto disposto dal Modello, dai suoi protocolli e dal Codice Etico;

b) omettano volutamente di rilevare o riportare eventuali violazioni o adottino – o minaccino di adottare – ritorsioni contro altri che riportano eventuali violazioni.

La Società adotterà adeguati provvedimenti disciplinari e sanzionatori anche nei confronti dei responsabili dei seguenti comportamenti illeciti:

a) ritorsioni;

b) ostacolo, anche solo tentato, alla segnalazione;

c) violazione dei doveri di riservatezza;

d) mancata istituzione dei canali di segnalazione;

e) adozione di procedure di segnalazione non conformi alle previsioni del D.Lgs. 231/2001 così come modificato dal D.Lgs 24/2023.

I provvedimenti disciplinari saranno proporzionati all'entità e gravità dei comportamenti illeciti accertati e potranno giungere fino alla risoluzione del contratto di lavoro.

CONSERVAZIONE DELLA DOCUMENTAZIONE

Tutte le Funzioni e gli organi coinvolti nelle attività disciplinate dalla procedura sulle segnalazioni assicurano, ciascuna per quanto di propria competenza e anche mediante i sistemi informativi utilizzati, la tracciabilità dei dati e delle informazioni e provvedono alla conservazione e archiviazione della documentazione prodotta, cartacea e/o elettronica, in modo da consentire la ricostruzione delle diverse fasi del processo stesso.

Al fine di garantire la gestione e la tracciabilità delle segnalazioni e delle relative attività, l'Ufficio Segnalazioni cura la predisposizione e l'aggiornamento di tutte le informazioni riguardanti le segnalazioni e assicura l'archiviazione di tutta la correlata documentazione di supporto per un periodo di cinque anni dalla ricezione.

6. IL REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI (GENERAL DATA PROTECTION REGULATION).

Una delle principali novità legislative del 2018, caratterizzate dalla decisiva influenza sulle procedure aziendali, è il nuovo regolamento europeo in materia di protezione dei dati personali, Regolamento Ue 2016/679, (GDPR, ossia "General Data Protection Regulation"), che deve essere obbligatoriamente applicato da tutti i soggetti destinatari, quali imprese, enti privati e pubblici, professionisti che hanno il dovere di garantire il massimo rispetto della normativa in materia di riservatezza e protezione dei dati personali.

Il GDPR è destinato a tutte quelle aziende che raccolgono e/o elaborano dati personali di cittadini europei e ha effetto anche se le imprese che possiedono i dati hanno sede al di fuori dei confini dell'UE, offrendo servizi o prodotti all'interno del mercato unico.

La nuova normativa si applica a tutte le aziende, ovunque stabilite, al fine di offrire una tutela diretta ai cittadini, imponendo alle aziende di adeguarsi alla nuova disciplina.

Rispetto alla precedente regolamentazione, il Regolamento impone alcuni adempimenti che consentono di implementare, completandolo, il sistema di trattamento e protezione dei dati già adottato dai soggetti obbligati. In particolare, le regole imposte dal nuovo regolamento possono essere così sintetizzate:

- definire una politica di conservazione dei dati;
- aggiornare le informative ai sensi dell'art. 13 del GDPR;
- verificare le condizioni di liceità dei trattamenti e delle fattispecie per cui è necessario richiedere il consenso (artt. da 6 a 10);
- revisionare i rapporti con tutti i responsabili esterni dei trattamenti (con ritrattazione degli obblighi previsti all'art. 28);
- revisionare/aggiornare l'analisi dei rischi per la definizione di misure di sicurezza adeguate (art. 32);
- per gli enti pubblici (e per i privati qualora ricorrano le condizioni di cui all'art. 37 comma 1), individuare e nominare un Data Protection Officer (DPO).

Il GDPR ha ampliato la definizione di dato personale e sensibile, che non è più riferito a dati quali indirizzo o numero di telefono, ma ricomprende anche i dati identificativi *online* come *cookie*, indirizzi IP, geolocalizzazione ed *email*.

Il Regolamento, infatti, individua quattro macro-categorie di interesse:

- dati personali: informazioni che identificano la persona, incluso nome, cognome, caratteristiche fisiche, identificativi online;
- dati genetici: dati ottenuti tramite analisi di DNA o RNA da un campione biologico;
- dati biometrici: caratteristiche fisiche identificative della persona, come l'impronta digitale, l'iride o l'immagine facciale;
- dati sulla salute: qualsiasi dato relativo alla salute, fisica o mentale.

Per adeguarsi al nuovo regolamento, nel raccogliere i dati, le aziende devono seguire le seguenti regole:

- permettere all'utente di fornire il proprio consenso in modo esplicito e tracciabile;
- predisporre un'informativa sul trattamento dei dati personali trasparente, chiara e facilmente accessibile;
- garantire che i dati raccolti siano pertinenti, adeguati e limitati alle finalità per cui vengono richiesti e trattati.

La richiesta di consenso deve essere chiara, comprensibile e deve essere presentata in una schermata facilmente riconoscibile. Bisogna, inoltre, garantire all'utente il diritto di revocare il proprio consenso in qualsiasi momento.

Emerge dunque una maggiore responsabilizzazione per le aziende, dovendo garantire la massima sicurezza dalla fase di raccolta sino a quella di elaborazione e conservazione dei dati.

Nel regolamento viene introdotto il diritto alla "portabilità" dei propri dati personali, pertanto viene concessa la possibilità a qualsiasi utente di trasferire i dati da un titolare del trattamento a un altro. Il cittadino, cioè, deve poter ottenere facilmente una copia dei propri dati personali, in un formato leggibile e facilmente trasferibile.

La norma trova un'eccezione nei casi i cui si tratta di dati contenuti in archivi pubblici, come ad esempio l'ufficio anagrafe; in questo caso il diritto non potrà essere esercitato.

Sono stati poi ampliati gli obblighi sussistenti in capo al Titolare e al Responsabile del trattamento (artt. 24 e ss..).

Essi non dovranno solo garantire il rispetto delle regole fissate per il trattamento dei dati personali, ma dovranno adottare una serie di misure giuridiche, organizzative e tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, adeguati al settore di interesse in cui svolge la propria attività.

Eventuali violazioni di dati personali vanno comunicate all'Autorità Garante da parte del Titolare del trattamento; il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Tra i principali obblighi cui le aziende devono attenersi vi è l'adozione del Registro dei trattamenti di dati personali (art. 30).

Il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare i danni; potrà decidere di non informarli qualora ritenga che la violazione non comporti un rischio elevato per i loro diritti o se dimostrerà di avere già adottato misure di sicurezza o ancora nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato al rischio.

L'Autorità Garante potrà imporre al titolare del trattamento di informare gli interessati, sulla base di una propria valutazione dei rischi correlati alla violazione commessa.

Tra i principali obblighi previsti dal nuovo regolamento europeo sulla *privacy* c'è quello, per alcune società, di adeguare il proprio organigramma *privacy* inserendo all'interno dello stesso la figura del DPO, *Data Protection Officer* (art. 37).

Il Responsabile della protezione dei dati personali, incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti, ha il compito principale del DPO di osservare, valutare e gestire i dati personali allo scopo di far rispettare le normative europee e nazionali in materia di *privacy*.

Il DPO è una figura professionale, con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi e dotato di conoscenze specialistiche della normativa e delle prassi in materia di protezione dati, nonché delle norme e delle procedure amministrative che caratterizzano il settore in cui opera.

Importante è garantire l'autonomia decisionale e l'estraneità del DPO rispetto alla determinazione delle finalità e delle modalità del trattamento dei dati; è tenuto in ogni caso al segreto e alla riservatezza in ordine alle sue funzioni di responsabile della protezione.

A seguito del recepimento del Regolamento UE sulla privacy, la società ha adottato una nuova procedura in linea con quanto prescritto dalla normativa, per il cui contenuto si rinvia al documento adottato.

7. SISTEMA DISCIPLINARE

FUNZIONE DEL SISTEMA DISCIPLINARE

L'art. 6, II comma, lett. e) e l'art. 7, IV comma, lett. b) del D.lgs. n. 231 del 2001 prevedono la necessaria adozione di "*un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello*", tanto nei confronti dei soggetti in posizione apicale, quanto verso i soggetti sottoposti all'altrui direzione. Per valersi dell'efficacia esimente del Modello, quindi, l'ente deve non solo adottare, ma anche efficacemente attuare un adeguato Sistema Disciplinare, nel caso in cui siano poste in essere violazioni del Codice Etico o delle procedure previste dal Modello.
Il Sistema Disciplinare ha una funzione preventiva, operando come presidio interno all'impresa, ed è diretto a contrastare comportamenti prodromici al reato. La sua inosservanza comporta l'attivazione del meccanismo sanzionatorio da esso previsto, indipendentemente dall'eventuale instaurazione di un giudizio penale per il reato eventualmente commesso.

INFORMAZIONE

Al fine di garantire la massima efficacia, il presente Sistema Disciplinare è pubblicato, nella sua versione completa, nella *intranet* aziendale e affisso presso le sedi della Società, in luogo accessibile a tutti. È, altresì, distribuito agli Amministratori, Sindaci, Organismo di Vigilanza, dipendenti, e portato a conoscenza dei Soggetti terzi. Sarà, poi, cura della Società informare i dipendenti, mediante comunicato interno, dell'approvazione del Sistema Disciplinare e della possibilità di prenderne visione presso gli uffici delle risorse umane.

REQUISITI DEL SISTEMA DISCIPLINARE

In accordo con le Linee guida per la costruzione dei Modelli redatte da Confindustria e seguendo le indicazioni dottrinali e giurisprudenziali sul punto (cfr. Corte cost., 29 maggio 1995, n. 220), il Sistema Disciplinare adottato da Rangers S.r.l. risponde a precisi requisiti:

- **Requisito dell'autonomia.** Il Sistema Disciplinare si aggiunge a quello esterno penale o amministrativo e mira a sanzionare le violazioni del Modello indipendentemente dal fatto che da esse sia scaturita la commissione di un reato.
- **Principio di tipicità.** Alla tipicità delle violazioni, segue il principio di tipicità delle sanzioni. Il Modello individua nel dettaglio le misure disciplinari da applicare a chiunque non osservi le misure organizzative adottate, ricollegando a ciascuna violazione o gruppo di violazioni le sanzioni applicabili, in una prospettiva di gravità crescente.
- **Forma scritta.** Il Sistema Disciplinare è redatto per iscritto e adeguatamente divulgato mediante una puntuale e capillare informazione e formazione dei destinatari.
- **Principio di proporzione.** Il potere disciplinare deve essere esercitato in modo coerente al fatto addebitato, per commisurare a esso, se ritenuto sussistente, la sanzione da irrogare,

parametrandola alla sua maggiore o minore gravità. Pertanto, non sono ammissibili meccanismi sanzionatori che non prevedono la possibilità di una graduazione secondo la gravità del fatto addebitato.

- **Principio del contraddittorio.** La valutazione dell'addebito, necessariamente prodromica all'esercizio del potere disciplinare, non è un mero processo interiore e interno a chi tale potere esercita, ma implica il coinvolgimento di chi versa nella situazione di soggezione, il quale – avendo conosciuto l'addebito per essergli stato previamente contestato – deve poter addurre in tempi ragionevoli, giustificazioni a sua difesa.

Per completezza espositiva va sottolineato che, sebbene molti dei principi che saranno di seguito richiamati sono espressamente enunciati solo in relazione al lavoro subordinato (art. 2106 c.c.; art. 7 L. 300/1970, recante il cd. Statuto dei Lavoratori), la giurisprudenza costituzionale ne ha sancito l'applicabilità nello svolgimento di qualsiasi rapporto di lavoro, anche autonomo o professionale

DESTINATARI

Sono tenuti all'osservanza delle prescrizioni del Modello e all'osservanza del Codice Etico, e sono quindi destinatari del presente Sistema Disciplinare:

a) i soggetti che nell'ambito della Società rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché di persone che esercitano, anche di fatto, la gestione e il controllo della stessa (soggetti apicali);
b) le persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale (dipendenti);
c) altri soggetti che, a vario titolo, intrattengono rapporti contrattuali con la Società od operano direttamente o indirettamente per essa (terzi destinatari).

COMPORTAMENTI SANZIONABILI

Costituiscono violazione del Modello e dei suoi protocolli:

a) la messa in atto di azioni o comportamenti non conformi alle prescrizioni o alle procedure previste o richiamante nel Modello, ovvero l'omissione di azioni o comportamenti prescritti o richiamati dal Modello, nell'espletamento di attività nel cui ambito ricorre il rischio di commissione dei reati contemplati dal D.lgs. 231/2001;
b) la messa in atto di azioni o comportamenti non conformi alle prescrizioni o alle procedure previste o richiamate nel Modello, ovvero l'omissione di azioni e comportamenti prescritti o richiamati dal Modello, nell'espletamento delle attività connesse ai processi sensibili che:
    - espongano la Società a una situazione oggettiva di rischio di commissione di uno dei reati contemplati dal D.lgs. 231/2001;
    - siano diretti in modo univoco al compimento di uno o più reati contemplati dal D.lgs. 231/2001;

- siano tali da determinare l'applicazione a carico della società di sanzioni previste dal D.lgs. 231/2001.

Costituiscono violazione del Codice Etico:

- la messa in atto di azioni o comportamenti non conformi ai principi contenuti o richiamati nel Codice Etico, ovvero l'omissione di azioni o comportamenti prescritti o richiamati dal Codice Etico, nell'espletamento dei processi sensibili o di attività connesse ai processi sensibili.

CRITERI DI SCELTA DELLE SANZIONI

Nell'irrogare le sanzioni si deve tenere conto della specifica idoneità di ciascuna in relazione alla natura e al grado di esigenze da soddisfare nel caso concreto.
In particolare, si dovrà tener conto di:

a) volontarietà o involontarietà del comportamento;
b) rilevanza degli obblighi violati;
c) gravità del pericolo creato alla Società;
d) entità del danno creato alla Società dall'eventualità applicazione delle sanzioni previste dal D.lgs. n. 231 del 2001 e successive modifiche e integrazioni;
e) livello di responsabilità gerarchica e/o specialistica;
f) presenza di circostanze aggravanti o attenuanti con particolare riguardo alle precedenti prestazioni lavorative e ai precedenti disciplinari negli ultimi cinque anni;
g) eventuale condivisione di responsabilità con altri lavoratori che abbiano concorso nel determinare la mancanza.

TIPOLOGIE DI SANZIONI APPLICABILI

SANZIONI NEI CONFRONTI DEI SOGGETTI APICALI

A seconda della gravità della infrazione e in considerazione della particolare natura del rapporto, il mancato rispetto delle prescrizioni da parte dei soggetti apicali è sanzionato, con i seguenti provvedimenti disciplinari:

<u>Amministratori, eventuali Procuratori e Sindaci:</u>

- **nota di biasimo**;
- **diffida scritta al puntuale rispetto delle previsioni del Modello**;
- **decurtazione degli emolumenti o del corrispettivo previsto fino al 50%**;
- **revoca dell'incarico**.

Quando le violazioni sono commesse dal Consiglio di Amministrazione o da uno dei suoi componenti, sarà l'Assemblea dei soci ad adottare il provvedimento, dandone comunicazione all'Organismo di Vigilanza. Laddove sia accertata la violazione da parte di un Sindaco, sarà il

Consiglio di Amministrazione ad adottare il provvedimento più opportuno rispetto al caso concreto, dandone tempestiva comunicazione all'OdV.

L'applicazione delle sanzioni disciplinari sopra citate, non esclude la facoltà della Società di promuovere l'azione di responsabilità, così come prevista dal codice civile.

Dirigenti apicali e Dirigenti con delega di funzioni *ex* art. 16 D.lgs. 81/08:

- **richiamo scritto, in caso di violazioni non gravi**. Per violazione non grave deve intendersi ogni violazione che non abbia prodotto danni e/o pregiudizi di qualunque tipo, compreso il pregiudizio all'immagine dell'ente e non abbia prodotto conseguenze nei rapporti con gli altri esponenti dell'ente stesso;
- **multa non superiore all'importo di quattro ore di retribuzione**, qualora sia commessa, entro un anno dall'applicazione del rimprovero scritto, altra irregolarità. Detto provvedimento si applica, altresì, nel caso di violazioni più gravi, sempre che da tale violazione non derivi un pregiudizio alla normale attività della Società;
- **licenziamento con preavviso**. Tale sanzione sarà comminata quando si commettono gravi infrazioni alla disciplina e alla diligenza del lavoro, quali possono essere quelle di seguito elencate, a titolo di riferimento, e che non siano coì gravi da rendere applicabile la sanzione del licenziamento senza preavviso:
    - quando, dalla violazione del Modello, dei suoi protocolli o del Codice, sia conseguito un danno patrimoniale per la Società o la stessa sia stata esposta a una situazione oggettiva di pericolo per la integrità dei beni aziendali o dell'immagine;
    - quando non avvertano tempestivamente i vertici di eventuali irregolarità, poste in essere da parte di sottoposti o appartenenti alla struttura di competenza, che determinino un danno patrimoniale alla Società o espongano la stessa a una situazione oggettiva di pericolo per la integrità dei beni aziendali o dell'immagine;
    - quando effettuino, con intenti fraudolenti, elusioni delle disposizioni e dei principi contenuti nel Modello, nei suoi protocolli e nel Codice;
- **licenziamento senza preavviso.** Tale sanzione sarà comminata quando i dirigenti apicali commettono infrazioni così gravi da ledere irreparabilmente il rapporto di fiducia e non consentire la prosecuzione nemmeno provvisoria del rapporto di lavoro o che commettono condotte che costituiscono reato.

SANZIONI NEI CONFRONTI DEI SOGGETTI SUBORDINATI

Ai dipendenti sottoposti alla direzione e alla vigilanza dei soggetti in posizione apicale che violano le prescrizioni del Modello e del Codice, ferma la preventiva contestazione e la procedura di cui all'art. 7 della L. n. 300/1970, sono irrogabili le sanzioni previste dal CCNL dei settori di appartenenza, nel rispetto del principio di gradualità della sanzione e di proporzionalità e offensività della gravità dell'infrazione.

In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale non possono essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa.

Nello specifico si applica:

- **rimprovero verbale,** quando si realizza una violazione di lieve entità delle procedure previste dal Modello o l'adozione di un comportamento non conforme alle prescrizioni del Modello medesimo;
- **ammonizione scritta,** si applica quando vi è la reiterata violazione di una lieve entità delle procedure interne previste dal Modello o l'adozione di un comportamento non conforme alle prescrizioni del Modello medesimo;
- **multa non superiore all'importo di quattro ore di retribuzione**, qualora sia commessa, entro un anno dall'applicazione del rimprovero scritto, altra irregolarità. Detto provvedimento si applica, altresì, nel caso di violazioni più gravi, sempre che da tale violazione non derivi un pregiudizio alla normale attività della Società. Il provvedimento è adottato dal dirigente responsabile della struttura alla quale il dipendente è assegnato nel momento in cui si verifica l'infrazione;
- **sospensione dal servizio e dalla retribuzione per un periodo massimo di 7 giorni**, qualora la violazione commessa determini un danno patrimoniale alla Società o esponga la stessa a una situazione oggettiva di pericolo per l'integrità dei beni aziendali. Tale provvedimento si applica, altresì, nei casi in cui, pur non trattandosi di infrazioni così gravi da rendere applicabile una maggiore sanzione, esse abbiano, comunque, rilievo tale da non trovare adeguata collocazione tra le violazioni descritte nei punti precedenti. La sanzione è comminata dal dirigente responsabile della struttura alla quale il dipendente è assegnato nel momento in cui si verifica l'infrazione, e ne viene data tempestiva comunicazione all'Amministratore Delegato;
- **licenziamento con preavviso**, in caso di grave violazione del Modello o del Codice tale da configurare un notevole inadempimento. Detto provvedimento è adottato dall'Amministratore Delegato;
- **licenziamento senza preavviso**, qualora la violazione commessa sia di gravità tale da ledere irrimediabilmente il rapporto di fiducia con la Società e da non consentire la prosecuzione anche provvisoria del rapporto di lavoro. Detto provvedimento è adottato dall'Amministratore Delegato.

SANZIONI NEI CONFRONTI DEI TERZI

L'inosservanza delle prescrizioni e delle procedure stabilite o richiamate nel Modello e nel Codice Etico da parte dei Soggetti Terzi può determinare, nei loro confronti ed in conformità a quanto disciplinato nello specifico rapporto contrattuale, le seguenti sanzioni:

- **diffida** al puntuale rispetto delle previsioni e dei principi stabiliti nel Codice Etico qualora la violazione di una o più regole comportamentali in esso previste configuri lieve irregolarità;

- **risoluzione del relativo contratto**, ferma restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D.lgs. n. 231 del 2001 qualora la violazione di una o più regole comportamentali previste nel Codice Etico determini un danno patrimoniale alla Società o esponga la stessa a una situazione oggettiva di pericolo per la integrità dei beni aziendali.

Nell'ambito dei rapporti con i terzi destinatari, la Società inserisce nelle lettere di incarico e/o negli accordi negoziali **apposite clausole** volte a prevedere, in caso di violazione del Modello, l'applicazione delle misure sopra indicate

MODALITÀ DI IRROGAZIONE DELLE SANZIONI

Il procedimento finalizzato all'applicazione di una sanzione disciplinare ha inizio con la rilevazione da parte dell'Organismo di Vigilanza di elementi idonei a configurare il pericolo di una violazione del Modello, acquisiti nell'espletamento della propria attività di vigilanza e verifica, o a seguito di segnalazione.

Il procedimento è caratterizzato da una prima fase c.d. **pre-istruttoria**, diretta a verificare la sussistenza della violazione. Tale fase è condotta dall'Organismo di Vigilanza che, per la valutazione delle violazioni scoperte o denunciate, può avvalersi, a seconda della loro natura, delle strutture interne della Società per lo svolgimento degli approfondimenti sui fatti oggetto del giudizio. Se la segnalazione ovvero la rilevazione dell'infrazione si dimostri infondata, l'OdV archivia il procedimento con motivazione che è riportata nella relazione annuale. In caso contrario, l'OdV deve compilare una relazione scritta contenente la descrizione della condotta contestata, l'indicazione delle previsioni del Modello che risultano violate, gli estremi del soggetto autore della violazione, eventuali documenti comprovanti la violazione e, infine, una propria proposta in merito alla sanzione più opportuna da comminare nel caso concreto. La relazione deve essere indirizzata al Presidente del Consiglio di Amministrazione e al Sindaco Unico quando la violazione sia stata realizzata da un soggetto in posizione apicale, al Datore di lavoro in caso di infrazioni dei soggetti in posizione subordinata.

Entro dieci giorni dalla relazione dell'OdV, gli organi competenti devono convocare tramite comunicazione scritta che dia certezza della data di ricevimento, il soggetto interessato dinanzi un'apposita commissione. Tale comunicazione deve contenere la contestazione della violazione che è mossa al soggetto e l'avviso che l'interessato può formulare eventuali rilievi, sia scritti che orali.

Si apre così la **fase istruttoria**, diretta ad accertare la fondatezza della violazione sulla base delle risultanze dell'OdV. La commissione deve essere riunita entro trenta giorni dalla ricezione della comunicazione da parte dell'OdV, e deve essere composta da almeno tre membri di cui il Presidente del Consiglio di Amministrazione, il componente dell'Organismo di Vigilanza, e il Sindaco Unico,

quando la violazione riguardi un apicale, il datore di lavoro, quando l'infrazione riguardi un subordinato.

In occasione dell'adunanza, vengono disposti l'audizione dell'interessato, l'acquisizione delle eventuali deduzioni da quest'ultimo formulate e l'espletamento degli eventuali ulteriori accertamenti ritenuti opportuni. Valutata la sanzione da proporre, il Presidente convoca il Consiglio di Amministrazione nei termini di Statuto per la decisione in ordine al provvedimento da assumere. Il Consiglio di Amministrazione, sulla scorta degli elementi acquisiti, determina la sanzione ritenuta applicabile, motivando l'eventuale dissenso rispetto alla proposta formulata dall'OdV.

8. SISTEMA DI FORMAZIONE E DIFFUSIONE DEL MODELLO

Per una piena efficacia del presente Modello e della corretta osservanza del Codice Etico deve essere svolta un'adeguata attività di diffusione di entrambi gli strumenti normativi, nonché di informazione e formazione nei confronti di tutto il personale della società, per favorire la conoscenza di quanto previsto dal D.lgs. 231/2001 e al Modello adottato nelle sue diverse componenti (mappatura delle aree/attività a rischio di reato, normativa e/o procedure che regolamentano le attività sensibili, Organismo di Vigilanza, flussi informativi e segnalazioni da parte dell'Organismo di Vigilanza, Sistema Disciplinare, Codice Etico).

INFORMAZIONE DEL PERSONALE/ DIFFUSIONE DEL MODELLO

Rangers S.r.l. si impegna a promuovere, nella propria attività di comunicazione interna (adeguata informativa nella lettera di assunzione per i neoassunti; spazio *intranet* dedicato al Modello e al Codice Etico) la più ampia informativa sulle tematiche legate alla prevenzione dei reati che possano comportare la responsabilità amministrativa ai sensi del Decreto 231.

Per tale ragione, viene garantita la divulgazione, attraverso diversi canali comunicativi , del presente Documento e del Codice Etico, con un diverso grado di approfondimento, in relazione al livello di coinvolgimento delle risorse umane nelle aree sensibili e strumentali alla potenziale commissione dei reati rilevanti per il Decreto 231.

La componente del Modello relativa al Sistema Disciplinare dovrà inoltre essere esposta nelle bacheche aziendali, così come previsto dall'art. 7 dello Statuto dei Lavoratori, Legge 20 Maggio 1970, n.300. Alle organizzazioni sindacali firmatarie del CCNL verrà inviata copia del Modello tramite raccomandata A.R.

Ai nuovi assunti deve essere consegnato un *set* informativo, con il quale assicurare loro le conoscenze considerate di primaria rilevanza. Tale *set* informativo deve contenere, oltre ai documenti di norma consegnati al neo-assunto, il Codice Etico,il Modello e il D.lgs.231/2001.

I dipendent sono tenuti a rilasciare alla Società una dichiarazione sottoscritta, ove si attesti la ricezione del *set* informativo nonché l'impegno a osservarne le prescrizioni.

È, inoltre, necessario prevedere analoga informativa e pubblicità del Modello per i collaboratori esterni (es. consulenti), nonché per i collaboratori a contratto, cosiddetti parasubordinati, e *outsourcer*, secondo modalità differenziate, in relazione alla possibilità di accesso alla normativa

aziendale, o attraverso consegna cartacea del Modello e del Codice Etico (con ricevuta di presa visione) ed eventualmente distinguendo, in relazione alla tipologia di rapporto contrattuale e alla tipologia di attività svolta in relazione ai rischi di reato presupposto del D.lgs.231/2001.

FORMAZIONE DEL PERSONALE

L'attività di formazione, finalizzata a diffondere la conoscenza della normativa di cui al D.lgs. 231/2001, è differenziata nei contenuti e nelle modalità di erogazione in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dei poteri e mansioni loro conferiti.

Il piano di formazione, in linea generale, prevede l'utilizzo di diverse modalità di erogazione, funzionali alla posizione – "apicale" o "subordinata" – dei destinatari e, soprattutto, del grado di rischio penale ipotizzato nell'area in cui operano (seminari mirati, prodotti *e-learning*, formazione in aula su specifici protocolli di prevenzione del rischio, ecc.).

La formazione, che può svolgersi anche a distanza o mediante l'utilizzo di sistemi informatici è operata da esperti nelle discipline dettate dal Decreto 231. La partecipazione alle attività di formazione rappresenta una condizione essenziale non solo a garanzia dell'effettiva attuazione del Modello, ma anche ai fini della corretta osservanza dello stesso, anche in relazione a quanto previsto dal sistema sanzionatorio.

La formazione è obbligatoria per tutti i livelli aziendali. Deve essere rilevata attestazione di frequenza dei corsi.

La formazione è programmata dalla Società in stretta cooperazione con l'Organismo di Vigilanza.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E DELLE LIBERALITA'

INDICE

1. FINALITÀ 2

2. IL SISTEMA DEI CONTROLLI 2

2.1. STANDARDDICONTROLLO GENERALI 2
2.2. STANDARD DI CONTROLLO SPECIFICI 3

3. AMBITO DI APPLICAZIONE 4

3.1 LE FUNZIONI AZIENDALI COINVOLTE 4

4. NORMATIVA DI RIFERIMENTO 5

5. REATI ASTRATTAMENTE PERPETRABILI 5

6. REGOLEGENERALI DI COMPORTAMENTO 11

7. PRESIDI DI CONTROLLO 13

7.1 GESTIONE DEI RAPPORTI CON LE PUBBLICHE AMMINISTRAZIONI 13
7.1.2 SPONSORIZZAZIONI 14
7.2 GESTIONE DEL CONTENZIOSO GIUDIZIALE E STRAGIUDIZIALE 26
7.3 LA SCHEDA DI EVIDENZA 27

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA 27

9. CONSERVAZIONE DELLA DOCUMENTAZIONE 28

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il personale deve attenersi nell'ambito del processo di "**Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità**".

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice Etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi Sociali, i Dipendenti, i Collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione de Modello;
- Fornire all'OdV e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi pe esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei Dipendenti – in via diretta – dei Collaboratori Esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione -di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da - considerati individualmente o collettivamente - integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee guida di Confindustria, nonché delle "*best practice*" prevede con riferimento alle Aree e alle Attività Sensibili individuate:

- *standard di controllo "generali"*, applicabili a tutte le Attività Sensibili;
- *standard di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

2.1. STANDARDDICONTROLLO GENERALI

I presidi di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:

- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;
- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa. Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

2.2. STANDARD DI CONTROLLO SPECIFICI

Sulla base dei presidi di controllo generali sopra riportati, quelli di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte

effettuate;

- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema delle deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

3. AMBITO DI APPLICAZIONE

Il presente Protocollo si applica a Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001, e concerne, in particolare, tutte quelle funzioni/uffici interessati e coinvolti nei processi di negoziazione e stipulazione di contratti con la Pubblica Amministrazione o che nell'espletamento dell'attività di propria competenza si trovino a dover gestire rapporti con la medesima Pubblica Amministrazione per:

- predisposizione di certificazioni e dichiarazioni;
- ottenimento di certificati, autorizzazioni e concessioni;
- comunicazioni di dati relativi all'attività (es. Questura, Prefettura, Banca d'Italia);
- comunicazioni di dati societari/aziendali di qualsiasi natura (es. Ufficio Catasto, Ufficio del Registro, Provincia, Agenzia delle Entrate);
- esecuzione dei servizi;
- gestione del contenzioso civile, amministrativo, penale e giuslavoristico;
- verifiche, ispezioni e accertamenti (es. ASL/Ufficio Ispezioni, Banca d'Italia, Vigili del Fuoco, UIF).
- gestione di regalie e omaggi a soggetti privati;
- erogazione di contributi a enti privati;
- sponsorizzazioni.

3.1 LE FUNZIONI AZIENDALI COINVOLTE

Le Funzioni/servizi/uffici aziendali coinvolti nelle attività sensibili sono:

- Ufficio Affari Legali Corporate;
- Direzione Acquisti Corporate;
- Ufficio Gare;
- Responsabile Controllo e Recupero Crediti;
- Direzione / funzione Risorse Umane Corporate;
- Direzione Commerciale;
- Responsabile Assistenza Tecnico/Commerciale;
- Back-office;
- Responsabile Operazioni;
- Responsabile Centrale Operativa;
- Responsabile Sviluppo Operativo;

- Responsabile di Filiale;
- Direzione Comunicazione e Marketing Corporate;
- Procuratore Speciale Gare;
- Responsabile di conformità per la prevenzione della corruzione (RAC).

4. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30"*;
- Legge 6 novembre 2012, n. 90 *"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"*.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;
- Protocollo su "Gestione degli Approvvigionamenti";
- Protocollo su "Selezione, assunzione e gestione del Personale e delle Guardie Particolari Giurate";
- Policy aziendale 4.2. – Gestione gare d'appalto;
- Istruzioni operative Ufficio contratti;
- Protocollo su "Gestione ed Esecuzione dei Servizi di Vigilanza e Trasporto";
- Codice Etico del Gruppo Battistolli;
- Manuale Antiriciclaggio;
- Organigramma aziendale;
- Procedure e istruzioni operative – Policy Gare;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Sistema di gestione di prevenzione della corruzione (UNI ISO 37001:2016);
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

5. REATI ASTRATTAMENTE PERPETRABILI

I reati presupposto di cui al D.lgs. 231/01 da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati.

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25):**

  - Malversazione di erogazioni pubbliche (art. 316-*bis* c.p.);

Il reato di malversazione a danno dello Stato si perfeziona quando s'impiegano contributi, sovvenzioni, mutui agevolati o finanziamenti pubblici (statali, di altri enti pubblici o comunitari) ottenuti per la realizzazione di opere e attività di vario genere, per finalità diverse da quelle per le quali sono stati erogati. L'ipotesi criminosa si caratterizza per l'ottenimento di finanziamenti pubblici in modo lecito e per il successivo utilizzo degli stessi per finalità diverse da quelle sottese all'erogazione. Il delitto può essere commesso da chiunque, estraneo alla P.A., ometta di destinare, anche parzialmente, i

Esempio: l'Azienda ottiene un finanziamento per lo svolgimento di un'attività di pubblico interesse. Le somme erogate vengono, tuttavia, destinate allo svolgimento di attività – pur conferenti con l'attività d'impresa esercitata dall'Azienda – ma diverse da quelle indicate nel finanziamento.

Al fine di contrastare la realizzazione di tale fattispecie di reato è prevista, quale standard di controllo di carattere generale, la segregazione delle attività: il soggetto che autorizza un'attività risulta diverso dal soggetto che la esegue e dal soggetto che, a sua volta, effettua un controllo, rendendo quantomeno conoscibile, all'interno dell'Azienda, eventuali distrazioni dei fondi ottenuti a titolo di finanziamento e responsabilizzando i vari soggetti nelle loro funzioni di controllori e controllati a catena; l'Organismo di Vigilanza, inoltre, deve essere informato della richiesta di finanziamenti ed ispeziona specificatamente il fascicolo della relativa procedura.

- Indebita percezione di erogazioni pubbliche (art. 316-*ter* c.p.);

Il reato in esame si concretizza nell'indebito conseguimento, per sé o per altri, di fondi, comunque denominati, concessi o erogati dallo Stato, da altri Enti pubblici o dalle Comunità europee, mediante l'utilizzo o nella presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero nella omissione di informazioni dovute. A differenza della malversazione, dunque, la fattispecie in esame riguarda il conseguimento indebito dei finanziamenti, senza che a nulla rilevi l'uso che poi venga fatto delle erogazioni. In breve, mentre la malversazione integra le ipotesi d'indebito utilizzo di fondi regolarmente erogati e conseguiti, l'art. 316 ter punisce le attività connesse a un momento precedente, ossia quello di un'indebita percezione dei fondi.

- Concussione (art. 317 c.p.);

Il reato di concussione si caratterizza per l'utilizzo indebito da parte del funzionario pubblico dei propri poteri, al fine di costringere il soggetto passivo a riconoscere al funzionario o ad un terzo soggetto un vantaggio di natura economica o personale. Si ha abuso dei poteri quando gli stessi siano esercitati fuori dei casi previsti da leggi, regolamenti e istruzioni di servizio o senza le forme prescritte, ovvero quando detti poteri, pur rientrando tra quelli attribuiti al pubblico ufficiale, vengano utilizzati per il raggiungimento di scopi illeciti.

- Truffa in danno dello Stato o di un ente pubblico (art. 640, comma 2, n. 1, c.p.);

L'ipotesi si configura nel caso in cui un qualunque soggetto, con artifici o raggiri tali da indurre in errore la controparte, procura a sè o ad altri un ingiusto profitto con danno dello Stato o di altro Ente pubblico. Trattasi di reato a dolo generico, sicché per la consumazione dello stesso è necessario che ricorrano tanto il profitto per il privato quanto il danno per lo Stato; l'assenza di tali elementi determina la necessaria qualificazione delle condotte fraudolente come ipotesi di truffa tentata e non consumata.

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

La fattispecie in oggetto consta dei medesimi elementi costitutivi della truffa semplice (art. 640 c.p.) ma rappresenta più grave ed autonoma fattispecie in quanto l'ingiusto profitto per il privato è rappresentato da contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri Enti pubblici o delle Comunità europee. Tale ipotesi si distingue dunque da quella prevista e punita ex art. 640, co. 2 n. 1 c.p. per la diversa natura del profitto, mentre si distingue dall'ipotesi di cui all'art. 316 ter c.p. per le diverse e più gravi modalità della condotta, che nella fattispecie in esame risulta più marcatamente connotata da comportamenti fraudolenti. Con la sentenza n. 5150/2013, la Corte di Cassazione ha affermato che in caso di procedimento "231" a seguito di truffa ai danni dello Stato per il conseguimento di pubbliche erogazioni, è legittimo il sequestro operato in capo al soggetto che, pur non essendo il diretto richiedente dell'erogazione, ne risulta il destinatario finale, in virtù di un rapporto a carattere privato con il ricevente principale. Segnatamente, il finanziamento pubblico era stato ricevuto da un soggetto privato che, mediante la sottoscrizione di contratti di appalto, lo ha a sua volta corrisposto alla società in questione. Tuttavia, secondo la Suprema Corte, la presenza di un "intermediario" non sarebbe sufficiente a far venir meno il carattere pubblico della somma di denaro.

- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.);

L'intervento manipolativo può essere tale da modificare gli scopi cui il sistema informatico è destinato, ma il reato ricorre anche quando - pur nel rispetto della destinazione del sistema - sono manipolati i contenuti dello stesso. Diversamente, la condotta alternativa di 'intervento abusivo' è rivolta ai dati, alle informazioni (cioè, per semplificare, ad un insieme di dati) o ai programmi (software) installati nell'hardware. In particolare, va rilevato che l'intervento, per configurare la condotta descritta dalla fattispecie ex art. 640 ter c.p., deve avvenire "senza diritto" e, dunque, non solo in assenza del necessario consenso del titolare dei dati, informazioni e programmi contenuti nel sistema informatico, ma anche secondo una modalità non consentita da norme giuridiche, né da altre fonti. Il reato di frode informatica presenta, in breve, la medesima struttura e i medesimi elementi costitutivi del reato di truffa da cui si distingue in quanto l'attività illecita investe non la persona ma un sistema informatico. Nel reato di frode informatica, pertanto, non assume rilevanza - a differenza che nel reato di truffa - il ricorso da parte dell'autore del reato ad artifizi o raggiri, ma l'elemento oggettivo dell'alterazione del sistema informatico (e/o dei dati in esso disponibili).

- Corruzione (artt. 318, 319, 320, 322-*bis* c.p.);

Il reato di corruzione consiste in un accordo fra un pubblico funzionario e un privato, in forza del quale il primo accetta dal secondo un compenso che non gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria). Nella corruzione il pubblico ufficiale ed il privato sono in posizione paritaria, diversamente dalla concussione che invece presuppone lo sfruttamento da parte del funzionario della propria posizione di superiorità alla quale corrisponde una situazione di soggezione nel privato. La fattispecie prevista dall'art. 319 c.p., connotata come quella di cui all'art. 318 c.p. da un rapporto paritetico tra pubblico ufficiale/ incaricato di un pubblico servizio-corrotto e privato-corruttore, se ne differenzia in virtù del fatto che l'atto richiesto al pubblico ufficiale o all'incaricato di un pubblico servizio a fronte della dazione o della promessa di denaro o di altra utilità, risulta contrario ai doveri d'ufficio. In particolare la condotta può concretizzarsi in una omissione o in un ritardo nel compimento di un atto di ufficio ovvero nel compimento di un atto contrario ai doveri di ufficio.

- Istigazione alla corruzione (art. 322 c.p.);

Il reato è configurabile solo ove l'offerta del privato o la richiesta del pubblico funzionario non vengano accolte dal destinatario. Tuttavia, ove il rifiuto non sia stato immediato e siano incorse trattative poi non sfociate in un accordo, si ritiene configurabile un tentativo di corruzione del quale rispondono entrambi i soggetti. Nell'istigazione alla corruzione passiva la condotta consiste nell'offrire o nel promettere denaro o altra utilità non dovuti al funzionario. L'offerta o la promessa deve essere seria e concreta ed idonea alla realizzazione dello scopo, tale cioè da indurre il destinatario a compiere o a ritardare un atto dell'ufficio o del servizio ovvero a fare un atto contrario a detti doveri. L'idoneità dell'offerta va valutata con un giudizio "ex ante" che tenga conto dell'entità del compenso, delle qualità personali del destinatario e della sua posizione economica e di ogni altra connotazione del caso concreto.

Esempio: il dipendente o l'amministratore dell'Azienda promettono denaro, omaggi o regali al funzionario pubblico al fine di aggiudicarsi una gara d'appalto o di far soprassedere, nelle svariate sedi, ad una visita ispettiva o al controllo di documentazione e certificazioni.

Al fine di contrastare la realizzazione di tale fattispecie di reato è stato inserito l'apposito presidio di controllo (7.1.1) facendo espresso divieto di offrire ed erogare denaro o altre utilità (dazioni, regalie, benefici diretti o indiretti, omaggi, atti di cortesia e di ospitalità) anche a seguito di illecite pressioni e/o a titolo personale, a Pubblici Ufficiali o a Incaricati di pubblico servizio con la finalità di promuovere o favorire gli interessi di Rangers S.r.l. o con lo scopo di indurli al compimento di un atto contrario ai propri doveri di ufficio. Inoltre è fatto obbligo, in situazioni di siffatto genere anche solo potenzialmente assimilabili ad episodi corruttivi in senso lato, di darne immediata segnalazione al Responsabile dell'Ufficio interessato e all'Organismo di Vigilanza.

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

Per quanto riguarda il reato di corruzione in atti giudiziari (art. 319 ter c.p.), si precisa che tale fattispecie non ricorre soltanto in relazione all'esercizio delle funzioni giudiziarie cui è subordinata e allo status di colui che le esercita, ma ha una portata più ampia. Infatti, come precisato dalla Corte di Cassazione, costituisce "atto giudiziario" qualsiasi atto funzionale a un procedimento giudiziario, indipendentemente dalla qualifica soggettiva di chi lo realizza (cfr. Cass., Sezioni Unite, sentenza n. 15.208 del 25/2/2010, con riferimento alla testimonianza resa in un processo penale).

- Corruzione tra privati (art. 2635 c.c.);

La nuova formulazione dell'art. 2635 c.c. estende il novero dei soggetti attivi includendo tra gli autori del reato, oltre a coloro che rivestono posizioni apicali di amministrazione o di controllo, anche coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive presso società o enti privati. Ai fini "231", per quanto concerne la corruzione tra privati, resta reato-presupposto la sola fattispecie di cui al comma 3 dell'articolo 2635 del codice civile, cioè il delitto commesso da chi corrompe, oggi anche per interposta persona, i soggetti indicati nel primo comma del medesimo articolo (nella sua nuova e più estesa versione) per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

- Istigazione alla corruzione tra privati (art. 2635 *bis* c.c.)

Diventa invece nuovo reato-presupposto anche l'istigazione alla corruzione tra privati (nuovo articolo 2635-bis comma 1). Anche in questo caso solo a carico della società alla quale appartiene il soggetto che istiga alla corruzione gli esponenti aziendali altrui, per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

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

Con l'introduzione di questa nuova fattispecie, in un'ottica di anticipazione della tutela, vengono incriminate condotte strumentali alla realizzazione di futuri accordi illeciti, in particolare punisce chi, sfruttando relazioni esistenti con pubblico ufficiale o incaricato di pubblico servizio, fa dare o promettere a sé o ad altri, indebitamente, denaro o altra utilità come prezzo della propria mediazione (a vantaggio dunque del mediatore) o, in alternativa, quale remunerazione destinata al pubblico ufficiale.

- Frode nelle pubbliche forniture (art. 356 c.p.);

Tale fattispecie punisce chiunque commette frode nell'esecuzione dei contratti di fornitura conclusi con lo Sato, con un Ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità. Per giurisprudenza e dottrina costante è richiesto un inadempimento dell'obbligazione parziale o inesatto ma anche in un adempimento totale. La condotta consiste nella frode nel corso dell'esecuzione di uno dei contratti indicati nell'art. 255 e pertanto devono riguardare cose od opere necessarie a unostabilimento pubblico o a un pubblico servizio.

- Peculato (art. 314, co. 1, c.p.);

Il reato si configura quando un pubblico ufficiale o un incaricato di un pubblico servizio si appropria di denaro o di altra cosa mobile altrui, di cui lo stesso è in possesso per ragione del suo ufficio o servizio. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

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

Il reato punisce il pubblico ufficiale o l'incaricato di un pubblico servizio, che, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

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

Tale reato punisce, salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

La fattispecie potrebbe realizzarsi, in concreto, nel caso in cui un dipendente dell'impresa, approfittando di rapporti personali con il funzionario pubblico preposto al rilascio di determinati permessi e/o autorizzazioni, prenda contatto con quest'ultimo per ottenere un provvedimento favorevole nell'interesse dell'impresa, pur consapevole di non averne diritto. Il dipendente (e con lui l'impresa nel cui interesse lo stesso abbia agito) risponderebbe a titolo di concorso dell'extraneus nel reato "proprio".

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

Tale fattispecie punisce chiunque, con violenza o minaccia o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni, ovvero ne allontana gli offerenti. Data la natura di reato di pericolo, esso si realizza indipendentemente dal risultato della gara, essendo per contro sufficiente che sia deviato il suo regolare svolgimento. Presupposto del reato è la pubblicazione del bando, non potendovi essere alcuna consumazione, neanche nella forma tentata, prima di tale momento.

- Turbata libertà del procedimento di scelta del contraente (art. 353 *bis* c.p.).

Tale fattispecie punisce, salvo che il fatto costituisca più grave reato, chiunque con violenza o minaccia o con doni, promesse, collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione. Con tale fattispecie, vengono incriminate le medesime condotte previste all'art. 353, con la differenza che la punibilità interviene già nella fase di predisposizione del bando e quindi nel momento in cui l'amministrazione interviene relativamente alle modalità di scelta del contraente. La norma in esame punisce, pertanto, le condotte prodromiche al compimento di atti in grado di turbare la libertà di scelta del contraente da parte della P.A., turbando il procedimento diretto a stabilire il contenuto del bando o di altro atto equipollente. Tale norma è stata introdotta con la finalità di fornire una specifica tutela anche alla fase di indizione della gara e, segnatamente, a quella di approvazione del bando, al fine di scoraggiare il comportamento di coloro che, con la collusione della stazione appaltante, tentano di far redigere i c.d. "bandi-fotografia" e cioè quei bandi di gara che contengono requisiti talmente stringenti da determinare *ex ante* la platea dei potenziali concorrenti.

- **Delitti di criminalità organizzata, introdotti dalla Legge 94/2009 (art. 24-*ter*):**
  - Associazione per delinquere, anche diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-*bis*, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286 (art 416 c.p.).

I delitti associativi in generale hanno carattere plurisoggettivo, ossia richiedono la partecipazione di almeno tre persone. La partecipazione può essere anche di secondaria importanza, purché il contributo sia apprezzabile, concreto e dotato di effettiva stabilità.Ai fini della configurabilità del delitto di associazione per delinquere, è necessaria la predisposizione di un'organizzazione strutturale, sia pure minima, di uomini e mezzi, funzionale alla realizzazione di una serie indeterminata di delitti, nella consapevolezza, da parte dei singoli associati, di far parte di un sodalizio durevole e di essere disponibili ad operare per l'attuazione del programma criminoso comune. In altre parole, l'art. 416 c.p. punisce coloro che promuovono, costituiscono o organizzano l'associazione allo scopo di commettere più delitti. Anche il solo fatto di partecipare all'associazione costituisce reato. La rilevanza penale delle condotte descritte dalla norma appare condizionata all'effettiva costituzione dell'associazione criminosa. Infatti, prima ancora di richiamare le singole condotte di promozione, costituzione, direzione, organizzazione ovvero di semplice partecipazione, la norma ne subordina la punibilità al momento in cui «tre o più persone» si siano effettivamente associate per commettere più delitti. Il delitto di associazione per delinquere si caratterizza quindi per l'autonomia dell'incriminazione rispetto agli eventuali reati successivamente commessi in attuazione del *pactum sceleris*. Tali eventuali delitti, infatti, concorrono con quello di associazione per delinquere e, se non perpetrati, lasciano sussistere il delitto previsto dall'art. 416 c.p. Al netto delle considerazioni sopra svolte, la configurazione dei reati associativi come reati-mezzo ha l'effetto di estendere la responsabilità dell'ente ex decreto 231 a una serie indefinita di fattispecie criminose commesse in attuazione del *pactum sceleris* e non necessariamente incluse nell'elenco dei reati presupposto.

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

6. REGOLEGENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici previsti dal Codice Etico, il Personale deve fare riferimento alle norme comportamentali di seguito individuate.

I rapporti con la Pubblica Amministrazione devono essere ispirati ai principi di correttezza, trasparenza ed efficienza e al pieno rispetto delle leggi e delle prescrizioni del Modello 231, dando puntuale e sollecita esecuzione alle prescrizioni e agli adempimenti richiesti.

Gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle normative vigenti (europee, nazionali, regionali, provinciali e comunali) e con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse. I documenti devono essere elaborati in modo puntuale e in un linguaggio chiaro, oggettivo ed esaustivo. Tutta la documentazione deve essere verificata e sottoscritta da parte di personale dotato di idonei poteri.
Le funzioni aziendali interessate devono dotarsi di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti nei confronti della Pubblica Amministrazione.
Quanto sopra si applica non solo nell'ambito degli ordinari rapporti con la Pubblica Amministrazione, ma anche nell'ambito di verifiche ispettive, procedure istruttorie e simili.

Inoltre, qualora il rapporto della Società con la Pubblica Amministrazione sia gestito anche attraverso professionisti esterni ovvero società di consulenza, agenti, ecc., i contratti e i conferimenti di incarico a tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e di impegno al suo rispetto.

Le modalità descritte sono obbligatorie sia nel corso della trattativa d'affari sia una volta che questa si è conclusa.

Tali regole trovano applicazione anche nei rapporti con l'Autorità giudiziaria, i suoi esponenti, ausiliari e consulenti.

Per quanto concerne la gestione delle liberalità, trovano applicazione i seguenti principi generali di comportamento.

Sono ammessi contributi e sponsorizzazioni ad associazioni senza fini di lucro e con regolari statuti e atti costitutivi che siano di elevato valore culturale o benefico.

L'attivazione di ciascuna erogazione è subordinata alla garanzia di congruità, adeguatezza e documentabilità della stessa.

Qualunque spesa ragionevole e in buona fede non deve consistere in un pagamento in contanti; deve essere legittima, effettuata in buona fede e in relazione a finalità di *business*; non deve essere motivata dalla volontà di esercitare un'influenza illecita o dall'aspettativa di reciprocità; deve essere

ragionevole secondo le circostanze e conforme agli *standard* di cortesia professionale generalmente accettati; deve, inoltre, rispettare le leggi e i regolamenti locali applicabili.

È possibile cooperare, anche finanziariamente, con le organizzazioni di cui sopra esclusivamente in relazione a specifici progetti che abbiano finalità riconducibili allo scopo sociale.

Le erogazioni devono essere mosse da spirito liberale, al fine di promuovere l'immagine della Società o per promuovere il progresso tecnico e il costante aggiornamento scientifico o per finalità riconducibili al *business* aziendale.

Il potere di decidere la politica aziendale in tema di omaggi e sponsorizzazioni e stanziare le relative finanze è esclusivo del Consiglio di Amministrazione.

Consegue un onere imprescindibile di documentazione delle spese effettuate e rendiconto trasparente delle stesse: devono essere registrate in maniera accurata e trasparente tra le informazioni finanziarie della Società con sufficiente dettaglio e supportate da documentazione di riferimento per individuare il nome e il titolo del soggetto emittente l'ordine di pagamento, il nome e il titolo di ciascun beneficiario del pagamento e lo scopo del pagamento stesso.

I pagamenti all'ente beneficiario devono essere effettuati esclusivamente sul conto registrato a nome dell'ente stesso; non è permesso effettuare pagamenti su conti cifrati o in contanti, a un soggetto diverso dall'ente beneficiario o in un Paese terzo diverso dal Paese dell'ente beneficiario. I contributi devono essere registrati in modo veritiero e trasparente nei libri e nei registri della Società.

La documentazione in originale relativa all'approvazione del contributo e i controlli di conformità con la relativa procedura devono essere conservati come previsto dalla normativa in tema di tenuta delle scritture contabili.

Non è consentito:

- promettere o offrire denaro, benefici, promesse di favori o altra utilità, anche sotto pressione psicologica o coercizione, anche se indirettamente, per tramite di interposta persona (es. agente, consulente, ecc.), a soggetti appartenenti alla Pubblica Amministrazione o a soggetti da questi segnalati con la finalità, anche implicita, di acquisire trattamenti di favore per sé o nella conduzione di qualsiasi attività collegabile alla Società (si rinvia al Protocollo "Gestione dei rapporti con la pubblica amministrazione");
- erogare alcuna elargizione che possa costituire, in maniera implicita o esplicita, un vincolo per l'Ente a prediligere prodotti o servizi della Società in fase di promozione e vendita degli stessi, né tantomeno che possa in alcun modo influenzare il giudizio del personale dell'Ente beneficiario;
- fare un utilizzo improprio degli strumenti di pagamento diversi dal contante;
- alterare, distrarre o mettere a disposizione d'altri gli strumenti di pagamento diversi dal contante;
- alterare i sistemi informatici al fine di modificare o alterare strumenti di pagamento diversi dal contante.

La Società condanna tramite l'applicazione del Sistema Sanzionatorio i comportamenti difformi ai principi sopra menzionati, così come previsti dal Codice Etico.

7. PRESIDI DI CONTROLLO

Le modalità operative che il personale della Società è tenuto a osservare per i processi sensibili nell'ambito delle attività di negoziazione e stipulazione di contratti sono di seguito descritte.

7.1 GESTIONE DEI RAPPORTI CON LE PUBBLICHE AMMINISTRAZIONI

Nell'ambito delle aree di attività che implicano rapporti con Pubblici Ufficiali, organi ispettivi, Enti pubblici erogatori di contributi e finanziamenti agevolati o titolari di poteri autorizzativi e concessori, sono state individuate le seguenti attività operative che, per peculiarità e svolgimento delle stesse, possono comportare la commissione di reati di cui agli artt. 24 e 25 del Decreto.

7.1.1 REGALIE E OMAGGI A SOGGETTI PUBBLICI O PRIVATI

È fatto divieto di offrire ed erogare denaro o altre utilità (dazioni, regalie, benefici diretti o indiretti, omaggi, atti di cortesia e di ospitalità), anche a seguito di illecite pressioni e/o a titolo personale, a Pubblici Ufficiali o a Incaricati di pubblico servizio con la finalità di promuovere o favorire gli interessi di Rangers S.r.l. o con lo scopo di indurli al compimento di un atto contrario ai propri doveri di ufficio. Questa regola di condotta non può essere elusa ricorrendo a forme di elargizione che, con apparenti diverse modalità (incarichi, consulenze, sponsorizzazioni, ecc.), abbiano la stessa finalità sopra vietata.

Qualunque spesa non deve in ogni caso consistere in un pagamento in contanti; deve essere legittima ed effettuata in buona fede;non deve essere motivata dal desiderio di esercitare un'influenza illecita o dall'aspettativa di reciprocità; deve essere ragionevole secondo le circostanze e conforme agli *standard* di cortesia professionale generalmente accettati; deve, inoltre, rispettare le leggi e i regolamenti applicabili anche specificamente alla P.A. interessata.

È comunque vietata ogni regalia effettuata su iniziativa personale o attingendo da fondi propri o sociali ma non preventivamente adibiti a tale scopo.

Il potere di decidere la politica aziendale in tema di doni e stanziare le relative finanze è in ogni caso esclusivo del Consiglio di Amministrazione.

Consegue un onere imprescindibile di documentazione delle spese effettuate e rendiconto trasparente delle stesse.

È sempre vietata ogni condotta sopra descritta (o analoga) compiuta su richiesta del Pubblico Ufficiale o dell'Incaricato di pubblico servizio: in caso di richiesta di tal fatta (sia essa diretta o indiretta, esplicita o implicita), i soggetti destinatari del presente Modello 231 sono tenuti a farne immediata segnalazione al Responsabile dell'Ufficio interessato e all'OdV, astenendosi da qualsivoglia attività nei confronti del Pubblico Ufficiale in questione.

Qualunque omaggio, ospitalità o altra utilità destinati a un familiare o a una persona indicata da un Pubblico Ufficiale e/o da un Incaricato di pubblico servizio su richiesta di quest'ultimo o in conseguenza del rapporto del Destinatario con lo stesso deve essere trattata come un'utilità al Pubblico Ufficiale e/o all'Incaricato di pubblico servizio, ed è pertanto proibita.

La Società non prevede l'erogazione di omaggi a soggetti terzi.
Tuttavia, in occasione della festività natalizia, di eventi (es. fiere, incontri stampa), o di altre iniziative poste in essere da parte della Società nelle proprie strategie commerciali, di *marketing* e di comunicazione, è prevista l'erogazione di beni di modico valore a titolo di omaggio a clienti, fornitori, e altri *partner* commerciali.
I beni omaggiabili devono avere carattere puramente simbolico ed essere di modico valore non eccedente le comuni pratiche commerciali.
Coerentemente con il *budget* annuale, nel quale è previsto un importo massimo erogabile approvato dal CdA, la Funzione Comunicazione e Marketing Corporate provvede a definire una proposta di selezione dell'oggettistica, sulla base del rapporto qualità/prezzo.
La quantità di beni da acquistare è definita in base a una lista di destinatari definita su indicazione dei Responsabili di Direzione e di Funzione, aggiornata dalla Funzione Comunicazione e Marketing e validata annualmente da parte del CdA.
La Funzione Comunicazione e Marketing Corporate ha la responsabilità dell'acquisto della merce, nel rispetto di quanto indicato nel protocollo "Acquisto di beni, servizi, consulenze e incarichi professionali", e della spedizione della stessa a destinazione.

7.1.2 SPONSORIZZAZIONI

Qualunque attività di sponsorizzazione deve essere formalmente autorizzata dal CdA e deve essere effettuata in coerenza con il *budget* approvato.
I *partner* in contratti di sponsorizzazione saranno soltanto enti o individui ben noti, affidabili e con un'eccellente reputazione in quanto a onestà e pratiche commerciali corrette.
Nel caso di società, il *partner* in un contratto di sponsorizzazione deve dimostrare di avere tutte le certificazioni e di aver soddisfatto tutti i requisiti per operare in conformità alle leggi applicabili.
Il contratto di sponsorizzazione deve essere redatto per iscritto.
Fatte salve le sponsorizzazioni rivolte a società sportive che rientrano nelle iniziative poste in essere dalla Società nelle proprie strategie commerciali, di *marketing* e di comunicazione, è richiesto alla Funzione Comunicazione e Immagine, di valutare l'iniziativa in base a:

- ritorno dell'iniziativa in termini di promozione dell'immagine del Gruppo e delle strutture organizzative/società richiedenti;
- rapporto tra il beneficio ottenuto dall'iniziativa e il costo sostenuto per realizzarla;
- rispondenza dell'iniziativa agli obiettivi di comunicazione;
- rispetto dei termini contrattuali previsti nella realizzazione della sponsorizzazione (es. la correttezza degli adempimenti convenuti, l'effettiva realizzazione delle attività secondo quanto indicato nella richiesta di sponsorizzazione).

In ogni caso, nella scelta delle proposte a cui aderire, la Società è attenta a prevenire e a evitare ogni possibile conflitto di interessi di ordine personale o aziendale.

L'ammontare pagato in coerenza con il contratto di sponsorizzazione deve essere registrato in modo veritiero e trasparente nei libri e registri della Società.
La Società deve assicurare che i pagamenti siano effettuati esclusivamente come indicato nel contratto di sponsorizzazione, previa verifica che il servizio sia stato effettivamente fornito.
La documentazione in originale relativa all'approvazione del contratto e i controlli di conformità con la relativa procedura devono essere conservati come previsto dalla normativa in tema di tenuta delle scritture contabili.

7.1.3 CONTRIBUTI A ORGANIZZAZIONIED ENTI PUBBLICI

Le donazioni a enti e organi amministrativi presentano il rischio che fondi o beni di valore siano distratti per uso personale o utilità di un Pubblico Ufficiale e/o Incaricato di pubblico servizio nell'esercizio delle sue funzioni o dei suoi poteri.

Rangers S.r.l. non fornisce alcun contributo, diretto o indiretto, sotto qualsiasi forma, a movimenti, partiti, comitati e organizzazioni politiche e sindacali, a loro rappresentanti e candidati, eccezion fatta per quanto ammesso e previsto dalle leggi e dai regolamenti vigenti. Si astiene, altresì, da qualsiasi pressione impropria, diretta o indiretta, nei confronti di esponenti politici e sindacali.

Qualunque contributo di beneficenza o donazione effettuato dalla Società deve essere formalmente stanziato dal CdA e deve essere versato in coerenza con il *budget* approvato. L'atto formale di stanziamento, adeguatamente motivato, deve essere trasmesso dal CdA all'OdV preventivamente alla sua esecuzione.

I pagamenti all'ente beneficiario devono essere effettuati esclusivamente sul conto registrato a nome dell'ente stesso; non è permesso effettuare pagamenti su conti cifrati o in contanti, a un soggetto diverso dall'ente beneficiario o in un Paese terzo diverso dal Paese dell'ente beneficiario. I contributi devono essere registrati in modo veritiero e trasparente nei libri e nei registri della Società.

La documentazione in originale relativa all'approvazione del contributo e i controlli di conformità con la relativa procedura devono essere conservati come previsto dalla normativa in tema di tenuta delle scritture contabili.

7.1.4 CONTATTI PERSONALI CON LE PUBBLICHE AMMINISTRAZIONI

Sono vietati contatti con le PP.AA. da parte dei soggetti a ciò non autorizzati dalla Società.

La Società assicura piena trasparenza e completezza informativa nella predisposizione di comunicazioni, prospetti e avvisi diretti alle Pubbliche Amministrazioni. È assolutamente vietato esibire a Pubblici Ufficiali documenti falsi o alterati, ovvero sottrarre od omettere l'esibizione, qualora dovuta, di documenti, informazioni o dati di qualsiasi tipo, ovvero dal tenere una condotta tendente a trarre in inganno le Pubbliche Amministrazioni.

Qualunque dipendente coinvolto nei contatti di cui sopra è tenuto a segnalare tempestivamente all'OdV ogni anomalia eventualmente insorta.

7.1.5 NEGOZIAZIONE/STIPULA E/O ESECUZIONE DI CONTRATTI/CONVENZIONI CON LE PP.AA. AI QUALI SI PERVIENE MEDIANTE PROCEDURE NEGOZIATE (AFFIDAMENTO DIRETTO O TRATTATIVA PRIVATA) O MEDIANTE PROCEDURE A EVIDENZA PUBBLICA (APERTE O RISTRETTE)

La Società, nelle attività di negoziazione, stipula ed esecuzione di contratti con la P.A. applica i seguenti princìpi:

- sono definiti con chiarezza ruoli e compiti delle figure aziendali responsabili della gestione dei rapporti con la P.A., prevedendo controlli (es. la compilazione di schede informative, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) in ordine alla regolarità e legittimità delle richieste di informazioni avanzate dalla Società nei confronti degli uffici competenti della P.A., ovvero delle richieste avanzate nei confronti della medesima Società da esponenti della P.A.;
- sono contemplati specifici flussi informativi tra le Funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- è individuato nel Responsabile dell'Ufficio Gare Corporate il soggetto interno quale responsabile della procedura;
- sono stabilite specifiche forme di riporto periodico dell'attività svolta sia verso l'OdV che verso il Responsabile interno competente a gestire tali rapporti;
- è contemplata la segregazione dei dati a disposizione dei soggetti titolari delle attività di predisposizione e presentazione dell'offerta, prevedendo specifiche forme di verifica della congruità della stessa, graduate in relazione alla tipologia e dimensione dell'attività da contrattualizzare;
- è introdotta, in sede di definizione dell'offerta, una verifica idonea a evitare il rischio di produzione alla P.A. di documenti incompleti o inesatti che attestino, contrariamente al vero, l'esistenza delle condizioni o dei requisiti essenziali per partecipare alla gara e/o per l'aggiudicazione dell'incarico attraverso altre procedure, ovvero che determinino il rischio di contestazioni da parte di terzi soggetti o varianti in corso d'opera;
- è prevista la trasmissione di dati e informazioni al Responsabile interno della commessa attraverso un sistema (anche informatico) che consente di tracciare i singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- è stabilita la segregazione delle attività di conclusione del contratto, di verifica della liquidazione e degli addebiti;
- sono definiti modalità e termini di gestione del rapporto contrattuale in essere, delle contestazioni del cliente, individuando le Funzioni responsabili della ricezione delle contestazioni, della verifica dell'effettività dell'oggetto del contendere, dell'effettuazione degli storni e della verifica degli stessi.

RAPPORTI CON I SOGGETTI CONCORRENTI

Nell'attività di negoziazione e/o stipula dei contratti con la P.A., la Società adotta misure di comportamento nei confronti dei *competitor,* volte a mitigare situazioni pregiudizievoli nella fase di individuazione dei contraenti da parte della Pubblica Amministrazione. In particolare, è fatto divieto a tutto il personale dipendente nonché a Procuratori e componenti del CdA, di:

- discutere di argomenti sensibili dal punto di vista della concorrenza sul mercato e/o scambiare informazioni sensibili con i concorrenti;
- inoltrare a un concorrente o a qualsiasi dipendente/collaboratore dello stesso gli annunci di incrementi di prezzo o i nuovi listini, anche se già adottati;
- contattare i concorrenti al fine di sondare la volontà di partecipare a gare d'appalto;
- confrontarsi con i concorrenti su eventuali scelte strategiche per partecipare alle gare d'appalto (es. sincronia nel rialzo delle tariffe, uniformazione delle condizioni commerciali, etc.);
- concordare con un concorrente o con qualsiasi dipendente e/o collaboratore dello stesso, misure e iniziative da intraprendere per impedire l'accesso al mercato di un nuovo soggetto concorrente.

Il rapporto con i *competitors* deve, pertanto, fondarsi sulla reciproca concorrenza leale sul mercato. A tal fine, quale esemplificazione delle condotte di "concorrenza sleale", la Società vieta qualsiasi forma di intesa con i soggetti concorrenti ivi inclusi gli accordi informali (ad esempio, verbalmente oppure attraverso uno scambio di e-mail, anche dai dipendenti che non hanno i necessari poteri per impegnare l'impresa verso terzi soggetti); i c.d. "*gentlemen's agreements*", o in ogni caso anche gli accordi giuridicamente non vincolanti. Sono vietate altresì le pratiche concordate, ossia quelle forme di coordinamento, che pur senza concretizzarsi in un vero e proprio accordo, costituiscono una consapevole collaborazione tra imprese a danno della concorrenza. I due elementi costitutivi essenziali della pratica concordata sono: (i) l'esistenza di qualche forma di contatto tra le imprese e (ii) un riscontro concreto della collaborazione sulle pratiche commerciali in concreto adottate.

È fatto, pertanto, divieto a qualsiasi Soggetto aziendale di instaurare intese con soggetti concorrenti aventi a oggetto, a titolo esemplificativo e non esaustivo:

- la fissazione in comune dei prezzi e/o delle altre condizioni commerciali (prezzi attuali o futuri, tempistica dell'aumento dei prezzi, livelli di sconto, criteri per l'ottenimento di sconti, margini di profitto, termini di pagamento; inserimento o non inserimento di clausole penali);
- l'adozione in comune di decisioni strategiche (accordi aventi ad oggetto la fissazione dell'ammontare degli investimenti, la tempistica/il lancio di nuovi servizi, la decisione di rifiutare il servizio a determinati tipi di clienti);
- l'allocazione/divisione di clienti (accordi aventi per oggetto la formulazione di proposte commerciali soltanto a clienti aventi determinate caratteristiche; la rinuncia alla formulazione di proposte commerciali a determinati clienti);
- l'allocazione/divisione di zone geografiche (accordi aventi per oggetto la rinuncia alla nomina di agenti commerciali/all'effettuazione di azioni pubblicitarie o promozioni in una determinata zona geografica; il rifiuto di ordini provenienti da clienti ubicati in una determinata area geografica; il trattamento differenziato di clienti a seconda della loro ubicazione);

- il c.d. *bid rigging*, ovverosia quando le imprese concorrenti in una gara pubblica o privata si accordano per determinarne in anticipo l'esito finale (accordi aventi ad oggetto: offerte "di comodo" o "in appoggio"; la mancata presentazione di un'offerta per favorire il vincitore designato; la rotazione delle offerte; l'assegnazione in subappalto di parte dei servizi all'impresa che ha rinunciato a partecipare alla gara).

La Società vieta, inoltre, qualsiasi comportamento che, pur non rientrando nel concetto di intesa o accordo, si concretizzi in condotte commerciali idonee a estromettere i concorrenti dal mercato o ad ostacolarne la possibilità di competere efficacemente. A titolo esemplificativo, sono vietati:

- i c.d. "sconti fedeltà", cioè quegli sconti subordinati all'impegno da parte dell'acquirente a non approvvigionarsi da imprese concorrenti;
- i c.d. "sconti *target*", cioè quegli sconti che sono subordinati al raggiungimento da parte dell'acquirente di un determinato obbiettivo di acquisto nel corso del periodo di riferimento;
- le pratiche c.d. "leganti", consistenti nel subordinare la vendita di un bene (generalmente quello in cui l'impresa è in posizione dominante), alla condizione che l'acquirente acquisti un altro prodotto o servizio economicamente separabile dal primo, senza che sussista l'esigenza di effettuare la vendita congiunta in quanto il prodotto o il servizio è commercializzabile separatamente;
- gli abusi da sfruttamento, cioè quelle condotte commerciali finalizzate a sfruttare il potere di mercato nei confronti dei contraenti al fine di estrarre profitti sovracompetitivi (es. discriminare gli acquirenti, applicando condizioni commerciali oggettivamente diverse per prestazioni equivalenti, sfruttando il diverso grado di preferenza/necessità degli acquirenti o imporre prezzi/condizioni contrattuali ingiustificatamente gravosi.

Nel caso in cui informazioni sensibili e confidenziali dal punto di vista della concorrenza sul mercato e/o proposte di intese/collaborazioni pervengano a dipendenti, Procuratori, Componenti del CdA, da parte del concorrente e/o da un Soggetto terzo, è fatto obbligo di non rispondere e non dar alcun seguito allo scambio informativo, segnalando con immediatezza l'accaduto all'Organismo di Vigilanza.

COSTITUZIONE CONSORZIO DI IMPRESE O ASSOCIAZIONE TEMPORANEA DI IMPRESE (ATI) – AVVALIMENTO

In fase di valutazione di convenienza alla partecipazione alla gara, i requisiti del bando possono essere tali da rendere opportuna la partecipazione congiunta in associazione con altre imprese attraverso la costituzione di un Consorzio di Imprese o di un'Associazione Temporanea di Imprese (ATI), ovvero formulare il solo impegno per una successiva costituzione a fronte di un'eventuale assegnazione della gara.

In tali casi il Responsabile Ufficio Gare, con il Procuratore Speciale Gare o con il Direttore di Divisione coinvolto ed eventualmente con l'Amministratore Delegato, si attiva per individuare e concordare le aziende con le quali partecipare e le quote di partecipazione.

Individuate le partecipanti, il Responsabile Ufficio Gare procede ai contatti con le stesse, alla verifica dei requisiti prescritti e alla successiva valutazione delle caratteristiche tecniche, economiche e finanziarie. In questa fase può avvalersi del supporto del Responsabile Tecnico Gare e Progettazione per richiesta di documentazione suppletiva.

A seguito di una valutazione di fattibilità, il Responsabile Ufficio Gare, sottopone il tutto al Procuratore Speciale Gare o al Direttore di Divisione o all'AD per la conferma a procedere. L'Ufficio Gare procede unitamente all'Ufficio Legale alla predisposizione di un impegno a costituirsi in ATI con le aziende partecipanti, con il relativo regolamento. In caso di procedura di Avvalimento è necessario predisporre apposito contratto.

Nell'ambito delle valutazioni richieste, l'Ufficio Gare, sulla base della documentazione di gara e delle informazioni giunte dagli Uffici coinvolti, provvede alla redazione degli atti necessari, eventualmente con la condivisione degli Uffici e/o delle Funzioni delle altre aziende coinvolte. La presente procedura varra` anche nel caso in cui le condizioni di gara siano tali per cui si debba ricorrere all'Istituto dell'Avvalimento.

LE FASI DEL PROCESSO DI PARTECIPAZIONE ALLE GARE D'APPALTO

Il processo di gestione delle gare d'appalto è suddiviso in tre fasi:

- Fase di *Scouting* e *Screening* Preliminare;
- Fase di Istruttoria di Gara;
- Fase di Valutazione Esito Gara

Si riportano indicazioni sintetiche in merito alle suddette fasi e si rinvia, per il resto, all'apposita *policy aziendale 4.2 – gestione gare d'appalto* adottata dalla società.

Tabella descrittiva: Fase *Scouting* e *Screening* Preliminare

Doc. Report	Ufficio/Funzione	Attività	Descrizione processo	Tempi
E-mail	Ufficio Gare	*Scouting* segnalazioni Gare, Richieste d'Offerta, Inviti a offrire	Effettua uno *scouting* dei Bandi di Gara, Richieste di Quotazione, Inviti a Offrire pubblicati utilizzando strumenti telematici oppure rilevando le segnalazioni inoltrate tramite e-mail	Giornalmente
E-mail	Ufficio Gare	*Screening* preliminare	Recupera informazioni in merito alle caratteristiche della gara di potenziale interesse e la documentazione disponibile (es. bando, disciplinare di gara, capitolato tecnico, allegati documentativi). Procede ad uno *screening* iniziale delle segnalazioni disponibili, rilevando i	entro 1 giorno dalla segnalazione

			termini di scadenza del bando e coinvolgendo il commerciale di riferimento per le valutazioni preliminari. ***NB:*** *In caso di tempistica stringente, è di fondamentale importanza, per una corretta gestione delle attività inerenti alla partecipazione alla Gara, dare opportuna segnalazione al Responsabile Ufficio Gare e al Direttore di Divisione o AD o Procuratore Speciale Gare di riferimento e a tutti gli Uffici* *coinvolti in modo che ognuno, nel proprio ambito, si attivi, anche con modalità di urgenza, per rispettare i termini di scadenza previsti dal bando stesso.*	
E-mail posta	Responsabile Tecnico Gare e Progettazione e Ufficio Personale	Analisi documentazione di Gara	Effettua un'analisi della documentazione di Gara se del caso con il supporto di consulenti esterni e, nel caso sia necessaria una personalizzazione, riepiloga le caratteristiche richieste dal servizio ed evidenzia tutte le criticità riscontrate ed i dubbi emersi all'Ufficio Gare, affinché contatti tutti gli Enti competenti e riceva risposte nei tempi utili per l'eventuale partecipazione alla Gara. Il Responsabile Tecnico Gare e Progettazione e Ufficio Personale, sulla base dei dati disponibili effettuano anche una prima valutazione di massima in merito all'incidenza economica dell'offerta Tecnica e del costo della Manodopera al fine di valutare l'effettiva presenza di un'accettabile marginalità, così da permettere a Direttori di divisione di competenza, o all'Amministratore delegato o al Procuratore Speciale Gare (nei limiti indicati in procura) di decidere sul GO o NO GO alla gara.	entro 3/5 giorni dalla segnalazione
E-mail	Tutti gli Uffici coinvolti	Analisi documentazione e verifica richieste	Effettuano un'analisi di fattibilità tecnica e legale e forniscono riscontro all'Ufficio gare, nelle tempistiche richieste caso per caso. Ogni funzione interessata effettua le verifiche di sua competenza e fornisce riscontro formale.	da 1 a 5 giorni
E-mail	Referenti per il sopralluogo	Effettuazione del sopralluogo e feedback	I referenti eventualmente delegati al sopralluogo riportano all'Ufficio Gare con apposita relazione scritta, segnalando eventuali criticità, in modo da consentire le valutazioni e gli approntamenti necessari alla partecipazione alla gara.	Entro 1 giorno dall'effettuazione del sopralluogo

E-mail	Ufficio Gare	Archiviazione e feedback	In caso di esito negativo dello *screening* iniziale o dell'analisi del Capitolato Tecnico, archivia la documentazione e fornisce un *report* all'Amministratore delegato al Direttore di Divisione o al Procuratore Speciale.	

Tabella descrittiva: Fase Istruttoria di Gara

Doc. report	Ufficio/Funzione	Attività	Descrizione processo	Tempi
E-mail	Ufficio gare	Avvio pratica di partecipazione a bando	L'Ufficio Gare inoltra la documentazione e le richieste di informazioni disponibili agli Uffici preposti affinché si attivino per le valutazioni di competenza e soprattutto per la predisposizione accurata dei documenti da produrre	Contestualmente all'esito della valutazione preliminare
E-mail	Ufficio gare	Coordinamento e raccolta pareri/ documentazione	L'Ufficio Gare, in maniera chiara e precisa, indica a tutti gli Uffici coinvolti, compreso il Risk Management, i tempi e le modalità entro le quali comunicare i *feedback* di ritorno, coordinando l'attività di raccolta della documentazione prodotta e da prodursi.	Contestualmente all'esito della valutazione preliminare
E-mail	Ufficio Legale	Verifica contenuti	L'Ufficio Legale, in caso di dubbi, funge da ausilio per la verifica dei contenuti dei documenti da produrre ricevuti dai singoli Uffici coinvolti e, se necessario, provvede a richiedere chiarimenti ai singoli Uffici ovvero a correggere eventuali errori.	Da 1 a 5 giorni
E-mail	Ufficio del Personale	Verifica contenuti	l'Ufficio del personale comunica al'Ufficio Gare il costo medio del personale da destinare al servizio con i dettagli delle voci costo che trovino adeguati giustificativi, oltre al costo in proiezione del personale coinvolto per tutta la durata dell'appalto con il riferimento alle caratteristiche specifiche e collocazione geografica della gara (cambio appalto, territorio, contratto applicabile, eventuali accordi di prossimità, etc...)	da 1 a 5 giorni
E-mail	AD / PSG / DD	Determinazione partecipazione	Nel caso di valutazione positiva da parte di tutti gli Uffici coinvolti, il Procuratore	da 1 a 5 giorni

			Speciale Gare o il Direttore di Divisione o l'AD, conferma per iscritto l'intenzione di partecipare alla gara	
E-mail	Ufficio gare	Raccolta, predisposizione ed invio documentazione di partecipazione	L'Ufficio Gare: Appronta la documentazione formale richiesta dal bando con il supporto di tutte le funzioni interessate; Sottopone la documentazione di gara al vaglio del Responsabile Ufficio Gare; Invia la documentazione di partecipazione, secondo le modalità e i tempi previsti dal bando.	Entro i termini di scadenza della gara

Tabella descrittiva: Fase valutazione esito gare

Doc. report	Ufficio/Funzione	Attività	Descrizione processo	Tempi
	Stazione Appaltante/Committente di Gara	Svolgimento Gara	La Stazione appaltante/o il Committente di gara procede alla valutazione delle offerte pervenute all'aggiudicazione della vincente. Comunica i risultati di gara secondo le modalità previste dalla gara stessa.	
	Responsabile Ufficio Gare	Rilevazione esito Gara	Il Responsabile Ufficio Gare decide se partecipare personalmente o a mezzo di delegato (con apposita procura/delega scritta) all'apertura delle buste.	Entro 24h da rilevazione esito gara
E-mail / posta elettronica certificata o equipollenti per l'accesso agli atti	Ufficio Gare	Comunicazione esito e predisposizione documentazione contrattuale	In caso di esito positivo della gara, l'Ufficio Gare, ricevuta la lettera di aggiudicazione della gara e il relativo contratto, comunicato formalmente l'esito positivo della partecipazione, effettua l'accesso agli atti della gara in relazione all'offerta tecnica e economica della seconda graduata e invia il contratto all'Ufficio Legale per la verifica delle clausole contrattuali e della documentazione ulteriore da produrre. L'Ufficio Gare verifica e predispone la documentazione propedeutica (giustificativi offerta anomala, comprova dei requisiti) alla sottoscrizione del contratto coinvolgendo gli uffici competenti.	Entro 24h da rilevazione esito gara
E-mail	Ufficio Gare	Verifica Documentazione integrativa o	Ove vengano segnalate difformità rispetto alla documentazione iniziale di gara, ovvero vengano	Compatibilmente con le difformità evidenziate

		nuova documentazione.	richiesti nuovi documenti, l'Ufficio Gare esamina nuovamente la documentazione e verifica se è compatibile con le condizioni accettate.	
E-mail	Ufficio Gare	Attivazione servizio.	Una volta ricevuto *feedback* positivi dagli uffici coinvolti, si provvederà alla firma del contratto da parte del Rappresentante legale dell'azienda, dando comunicazione agli Uffici operativi per la preparazione della esecuzione del servizio, secondo i tempi e le modalità previste dal contratto.	Secondo i termini previsti
E-mail/reporting/comunicazioni telefoniche	Responsabile di Filiale o back office	Esecuzione del contratto	In fase di esecuzione del servizio, il Responsabile di Filiale o il back office curerà tutti gli aspetti relativi alla esecuzione del contratto e ai rapporti con la Stazione Appaltante.	Per tutta la durata del contratto
E-mail	Ufficio gare	Archiviazione Documentazione	L'Ufficio Gare provvede ad archiviare tutta la documentazione prodotta per la partecipazione alla gara, indipendentemente dall'esito della stessa	
Posta elettronica certificata o equipollenti	Ufficio Gare	Accesso agli atti in caso di mancata aggiudicazione.	In tutti i casi in cui la Società del Gruppo Battistolli interessata risulti seconda o terza in graduatoria e, nelle altre ipotesi, se ne venga comunque ravvisata la necessità o l'opportunità dal Direttore di Divisione o dal Procuratore Speciale o dall''AD in relazione all'importanza e alla complessità della gara	Entro 24 h dalla comunicazione o notizia della mancata aggiudicazione se anteriore
e-mail	Ufficio Gare – Responsabile Tecnico Gare e Progettazione e Ufficio Amministrazione Gare	Esame documentazione di gara delle concorrenti	Analizza e riporta brevemente, le eventuali anomalie / incongruità delle offerte tecniche ed economiche presentate dalle imprese concorrenti; riportano ogni evidenza di elementi utili a potenziali motivi di ricorso in considerazione di eventuali erronee attribuzioni di punteggi e/o carenze, nella documentazione dell'aggiudicatario, relativamente ai requisiti indicati dagli atti di gara.	Entro 1-2 giorni dal ricevimento dei documenti e in ogni caso nei termini prestabiliti al fine di predisporre eventuali azioni giudiziarie

e-mail	Ufficio Legale	Feedback ad AD/PSG/DD	Vaglia con il consulente esterno la possibilità di presentare ricorso, mediante un approfondimento degli elementi oggetto di relazione anche in termini di costi / benefici; l'esito delle verifiche viene riportato a AD/PSG/DD	Entro 1-2 giorni dal ricevimento dei feedback da Ufficio Gare
e-mail	AD/PSG/DD	Incarico ricorso	Il Direttore di Divisione o l'AD o il Procuratore Speciale, in presenza di possibili elementi per il ricorso, considerati i tutti gli elementi utili nel rispetto dei termini normativi entro i quali predisporre la documentazione necessaria alla proposizione di eventuali azioni giudiziarie, incaricherà l'Ufficio Legale di predisporre l'eventuale ricorso nel rispetto dei termini utili previsti dalla legge. Nel caso in cui l'eventuale azione giudiziaria coinvolga necessariamente più aziende del Gruppo (ATI), la decisione finale sarà condivisa dai rispettivi AD/PSG/DD in relazione alle specifiche competenze.	Da 1 a 2 giorni e comunque in modo da garantire il rispetto dei termini normativi

7.1.6 ACQUISIZIONE E/O GESTIONE DI CONTRIBUTI, SOVVENZIONI, FINANZIAMENTI, O ALTRE EROGAZIONI DELLO STESSO TIPO COMUNQUE DENOMINATE

Con riferimento alle negoziazioni con le PP.AA. e alla partecipazione a bandi di gara per l'ottenimento di finanziamenti, contributi ed erogazioni pubbliche, il personale è tenuto a:

- operare seguendo i principi di correttezza, trasparenza e buona fede;
- valutare la congruità e la fattibilità delle prestazioni previste nel bando di gara;
- intrattenere relazioni trasparenti e corrette con i funzionari delle PP.AA.;
- adempiere alle obbligazioni contrattuali in modo diligente e puntuale.

Con riferimento all'erogazione di fondi pubblici, il Personale deve astenersi:

- dall'utilizzo di dichiarazioni attestanti fatti e notizie non veritiere, ovvero omettere informazioni per conseguire, a vantaggio e nell'interesse proprio o della Società, contributi, finanziamenti o altre erogazioni concessi, a qualsiasi titolo, dalle PP.AA.;
- dall'utilizzo di contributi, finanziamenti e altre erogazioni concesse dalla P.A. per finalità diverse da quelle per le quali erano stati assegnati.

È predisposto un fascicolo contenente:

- gli estremi della richiesta;
- lo stato di avanzamento della stessa;
- il nominativo e la sottoscrizione della persona fisica che si occupa della predisposizione della richiesta;
- il nominativo e la sottoscrizione della persona fisica che si occupa della firma della richiesta;
- tutta la documentazione concernente la richiesta (bando, certificazioni, dichiarazioni, ecc.).

L'Organismo di Vigilanza deve essere tempestivamente informato della richiesta di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, attraverso apposita nota informativa. È tenuto, inoltre, all'ispezione del fascicolo all'uopo predisposto.

Il soggetto richiedente verifica ed è responsabile della veridicità di quanto autocertificato mediante conservazione nel fascicolo della documentazione comprovante i dati autocertificati. L'Ufficio Affari Legali effettua controlli a campione sulle richieste effettuate.

In caso di anomalia, l'*iter* di richiesta deve essere sospeso e la problematica deve essere segnalata all'OdV.

In caso di aggiudicazione di finanziamento, occorre garantire il chiaro e corretto svolgimento di quanto previsto dal bando e il diligente e puntuale adempimento degli obblighi contrattuali, anche nei confronti di terze parti coinvolte.

La spendita di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea deve avvenire sempre e solo mediante operazioni conformi a quanto previsto dal Modello 231 e dai Protocolli operativi e per il solo fine per cui sono stati erogati.

A tali operazioni deve sempre seguire nota informativa da inserirsi nel fascicolo costituito in fase di richiesta contenente:

- attestazione del permanere delle condizioni e dei presupposti indicati dalla normativa che legittimano l'erogazione;
- rendiconto dell'impiego delle somme ottenute;
- indicazione di eventuali collaboratori esterni incaricati.

L'OdV controlla la completezza e la veridicità della documentazione e cura l'*iter* per l'utilizzo dei fondi.

7.1.7 GESTIONE DELLE VISITE ISPETTIVE

In caso di ispezioni, accessi e/o controlli da parte di soggetti pubblici e autorità di vigilanza è fatto obbligo di avvisare e attendere il responsabile dell'area coinvolta ovvero, qualora non disponibile, il Responsabile di Filiale.

Durante le visite ispettive, il personale deve astenersi dall'utilizzo di dichiarazioni attestanti fatti e notizie non veritiere, dalla presentazione di documenti alterati ovvero omettere informazioni per conseguire un vantaggio per sé o per la Società.

In presenza di richieste verbali da parte di Pubblici Ufficiali, è fatto obbligo di richiedere agli stessi di formalizzare per iscritto la richiesta; va altresì richiesta copia del rapporto e/o verbale eventualmente rilasciato dai Pubblici Ufficiali.

È obbligatorio documentare l'avvenuta ispezione e/o controllo compilando un *report* contenente:

- data dell'accesso;
- soggetti presenti all'accesso;
- generalità del funzionario intervenuto;
- motivo dell'intervento;
- descrizione sommaria delle attività svolte dal funzionario intervenuto;
- eventuali segnalazioni.

Tale *report* e il verbale e/o rapporto rilasciato dal funzionario intervenuto devono essere conservati agli atti della Società e trasmessi senza indugio all'Ufficio Legale, al *Risk Manager* e all'OdV.

In caso di richiesta scritta o qualsivoglia attività esulante l'ordinaria amministrazione coinvolgenti Enti Pubblici, ciascun dipendente è tenuto a farne immediata comunicazione all'OdV. Tale comunicazione non assolve agli altri eventuali obblighi previsti nel Modello 231, nei suoi Protocolli applicativi e nel Codice Etico.

7.2 GESTIONE DEL CONTENZIOSO GIUDIZIALE E STRAGIUDIZIALE

Per la gestione del contenzioso giudiziale e stragiudiziale occorre:

- individuare le Funzioni/Uffici responsabili della ricezione delle contestazioni, della verifica dell'effettività dell'oggetto del contendere, della gestione del contenzioso in fase stragiudiziale e della gestione del contenzioso in fase giudiziale;

- regolare le modalità e i termini per la repentina trasmissione della contestazione al legale incaricato, unitamente a una relazione illustrativa delle circostanze di fatto sulla cui base si poggia la suddetta contestazione;
- predisporre specifici flussi informativi tra i comparti aziendali coinvolti nell'attività sensibile con finalità di verifica e coordinamento reciproco;
- prevedere specifiche linee di *reporting* coordinate dall'Ufficio Affari Legali Corporate su base annuale, verso l'OdV sullo stato della vertenza e sulle possibilità e sui termini di definizione stragiudiziale o di conciliazione giudiziale della stessa;
- prevedere che il ricorso all'Autorità Giudiziaria sia basato su parametri oggettivi e che l'eventuale transazione e/o conciliazione venga condotta da Soggetto titolare di un'apposita procura e delega *ad litem*, che contempli il potere di conciliare o transigere la controversia.

7.3 LA SCHEDA DI EVIDENZA

Per ogni singola operazione attinente il processo "Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità" deve essere compilata dal responsabile interno un'apposita "Scheda di Evidenza" (All. 2) da tenere aggiornata nel corso dello svolgimento dell'operazione, all'interno della quale vanno descritti tutti i passaggi dell'attività svolta, e in particolare:

1. la descrizione dell'operazione a rischio con l'indicazione del valore economico dell'operazione;
2. la P.A. che ha competenza sulla procedura;
3. il nome del responsabile interno dell'operazione;
4. l'indicazione di eventuali collaboratori incaricati di assistere la Società nella partecipazione alla procedura;
5. l'indicazione di eventuali *partner* individuati ai fini della partecipazione congiunta alla procedura;
6. la dichiarazione rilasciata dai suddetti *partner* commerciali da cui risulti il reciproco impegno al rispetto dei princìpi di trasparenza e di correttezza e all'osservanza delle disposizioni di legge nella conduzione dell'operazione;
7. in relazione a visite, ispezioni e accertamenti avviati da parte di Enti pubblici e Autorità di vigilanza, l'attività svolta nel corso dell'ispezione, contenente, tra l'altro, i nominativi dei funzionari incontrati, la documentazione richiesta e/o consegnata, i soggetti coinvolti e una sintesi delle informazioni verbali richieste e/o fornite.

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni/Uffici interessati e, più in generale, i soggetti muniti di poteri in base al sistema di deleghe e procure sono tenuti a inoltrare all'Organismo di Vigilanza, con periodicità definita dallo stesso, adeguati *report* e relazioni mediante un sistema di flussi informativi volto a garantire il costante monitoraggio delle azioni intraprese.

In particolare, i Responsabili di Funzione/Uffici sono tenuti a inviare all'OdV, con cadenza annuale, relazioni inerenti l'attività svolta, nonché a inoltrare adeguate e specifiche segnalazioni ogni qualvolta si evidenzi una criticità nell'esercizio dell'attività del proprio Ufficio/Funzione. Qualunque altro soggetto coinvolto nei processi aziendali di cui sopra, laddove se ne ravvisi la necessità, è tenuto a inoltrare, senza ritardo, specifica segnalazione all'OdV.

Conformemente a quanto stabilito nella Parte Generale del Modello, fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli di propria iniziativa o a seguito delle segnalazioni ricevute, esso effettua periodicamente controlli a campione sulle attività di "Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità", diretti a verificare l'applicazione dei protocolli di prevenzione in conformità a quanto sopra previsto.

9. CONSERVAZIONE DELLA DOCUMENTAZIONE

I Responsabili delle Funzioni/Uffici coinvolti nei processi sensibili individuati nel presente Protocollo operativo sono responsabili, ciascuno per la parte di propria competenza, della conservazione della documentazione, nel rispetto dei termini di legge, al fine di garantire la tracciabilità delle operazioni aziendali. La documentazione è, inoltre, messa a disposizione, su richiesta, del Consiglio di Amministrazione, del Sindaco Unico e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

GESTIONE DEGLI APPROVVIGIONAMENTI

INDICE

1. FINALITÀ 2

2. AMBITO DI APPLICAZIONE 2

2.1 LE ATTIVITÀ A POTENZIALE "RISCHIO REATO" 2
2.2 LE FUNZIONI AZIENDALI COINVOLTE 3

3. NORMATIVA DI RIFERIMENTO 3

4. REATI ASTRATTAMENTE PERPETRABILI 4

5. REGOLE GENERALI DI COMPORTAMENTO 12

6. IL SISTEMA DEI CONTROLLI 13

6.1 STANDARD DI CONTROLLO "GENERALI" 14
6.2 STANDARD DI CONTROLLO SPECIFICI 14

7. GESTIONE DELLE FORNITURE DI BENI E SERVIZI 15

7.1. SELEZIONE DEI FORNITORI DI BENI E SERVIZI 15
7.2 PROCESSO DI APPROVVIGIONAMENTO DI BENI E SERVIZI 18
7.3 GESTIONE DEI RAPPORTI CONSULENZIALI 24
7.4GESTIONE DEI CORRISPONDENTI 25

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA 26

9. CONSERVAZIONE DELLA DOCUMENTAZIONE 26

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il personale deve attenersi nell'ambito del processo di "**Gestione degli approvvigionamenti**".

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società, nelle procedure e istruzioni operative, e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi sociali, i dipendenti, i collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle altre Funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei dipendenti – in via diretta – e dei collaboratori esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione – di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da – considerati individualmente o collettivamente – integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. AMBITO DI APPLICAZIONE

2.1 LE ATTIVITÀ A POTENZIALE "RISCHIO REATO"

Il presente Protocollo si applica alla società Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 e concerne, in particolare, tutte quelle Funzioni e unità operative coinvolte nelle seguenti attività:

- Ricerca e selezione dei fornitori/consulenti;
- gestione del processo di qualifica e valutazione del fornitore/consulente;
- gestione ed emissione degli ordini di acquisto/contratti;
- formalizzazione dei rapporti con i consulenti/fornitori di servizi;
- verifica e monitoraggio delle prestazioni rispetto al contratto/ordine;
- monitoraggio delle merci/servizi ricevuti in conformità con l'ordine di acquisto/contratto;
- gestione del rapporto con i consulenti;
- gestione dei rapporti con gli intermediari commerciali;

- gestione dei corrispondenti.

2.2 LE FUNZIONI AZIENDALI COINVOLTE

Le Funzioni aziendali che operano nell'ambito delle aree a rischio reato e delle attività sensibili sono:

- Ufficio Acquisti Corporate;
- Ufficio Automezzi e Vestiario Corporate;
- Responsabile Gestione Qualità;
- Responsabile Funzione;
- Funzione richiedente l'acquisto;
- Responsabile Operativo;
- Responsabile Assistenza Tecnico/Commerciale;
- Direttore di Divisione;
- Amministratore delegato;
- Risk manager;
- Responsabile IT;
- Datore di lavoro o suo delegato;
- Direzione Commerciale;
- Responsabile di conformità per la prevenzione della corruzione (RAC);
- Ufficio Corrispondenti.

3. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30"*;

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;
- Protocollo "Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità";
- Protocollo "Gestione delle operazioni e degli adempimenti fiscali";
- Codice Etico del Gruppo Battistolli;
- Policy approvvigionamenti di beni, materiali, servizi e manutenzioni (v. 2.3);
- Procedure e istruzioni operative;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Sistema di Gestione UNI EN ISO 9001:2015;
- Sistema di gestione di prevenzione della corruzione (UNI ISO 37001:2016);
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

4. REATI ASTRATTAMENTE PERPETRABILI

I reati presupposto (nella forma consumata o tentata) di cui al D.lgs. 231/01 da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati.

- **Reati in materia di ricettazione, riciclaggio e impiego di denaro di provenienza illecita, introdotti dal D.lgs. 231/2007 (art. 25-*octies*):**
  - Ricettazione (art. 648 c.p.);

La norma, in relazione al soggetto attivo, esclude che possa essere autore della ricettazione colui che ha commesso il reato da cui i beni provengono. Dunque, chi commissiona il delitto presupposto concorre nella sua realizzazione come istigatore ed è punibile a tale titolo, mentre la successiva condotta di ricezione rileva come mero post factum non punibile. L'oggetto materiale è costituito da denaro o cose provenienti da delitto. La giurisprudenza vi comprende i servizi, l'energia o programmi di *know how*, mentre si divide riguardo gli immobili. Infine, riguardo ai rapporti con le figure concorrenti, si può tendenzialmente affermare che la ricettazione è destinata a lasciare spazio alle previsioni che incriminano specificamente la ricezione di un determinato bene di origine illecita. Ad esempio, in applicazione del principio di specialità *ex* art. 15 c.p., gli artt. 453, n. 3/4 e 455 c.p., che sanzionano chi acquista, riceve o detiene monete contraffate o alterate al fine di metterle in circolazione, sono destinati a prevalere sull'art. 648 c.p.

Esempio: al fine di realizzare un risparmio di spesa, si decide di acquistare le armi in dotazione al personale servendosi di canali "non ufficiali", acquistando armi con matricola abrasa, non dotate di relativa certificazione o di dubbia provenienza.

  - Riciclaggio (art. 648-*bis* c.p.);

Anche ai fini della configurabilità del reato di riciclaggio è necessario che sia in precedenza consumata altra fattispecie criminale. Più precisamente, affinché vi sia un provento illecito da riciclare – sia esso denaro o altro bene o utilità – è imprescindibile il fatto che un reato, per l'appunto presupposto, sia stato commesso. Il riciclaggio consiste, quindi, nelle attività volte a dissimulare l'origine illecita dei proventi criminali ed a creare l'apparenza che la loro origine sia lecita.

Esempio: nelle normali operazioni di acquisto di automezzi per lo svolgimento delle attività aziendali, al fine di sostituire auto irrimediabilmente guaste, si acquistano autovetture di dubbia provenienza – a prezzi particolarmente concorrenziali – non dotate della targa e si provvede all'apposizione delle vecchie targhe già in possesso dell'Azienda per i vecchi mezzi.

Al fine di evitare la realizzazione di tali fattispecie di reato (ricettazione e riciclaggio) sui cui confini c'è fervente giurisprudenza, a titolo esemplificativo, si è predisposta una segregazione delle funzioni che sancisca una non identità tra chi richiede, chi dispone e chi autorizza un acquisto, una fornitura o comunque una spesa.

Caso specifico per l'integrazione del reato di riciclaggio, e non configurabilità della ricettazione, Cassazione Penale,Sez. 2, Sentenza n. 39702 del 17/05/2018 Ud. (dep. 04/09/2018). Rv. 273899 - 01

  - Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);

Chi impiega denaro di provenienza delittuosa, direttamente in un'attività economica o finanziaria, così ripulendolo, risponde non del reato di riciclaggio, ma di quello punito dall'art. 648-ter c.p. appunto «Impiego di denaro, beni o utilità di provenienza illecita». In quest'ultimo, infatti, è "assorbita" la precedente attività di sostituzione o di ricezione. Invece, se taluno sostituisce denaro di provenienza illecita con altro denaro o altre unità e, poi, impieghi i proventi derivanti da tale opera di ripulitura in attività economiche o finanziarie, risponde del solo reato di riciclaggio (art. 648 bis c.p.) con esclusione del 648-ter c.p.

- Autoriciclaggio (art. 648-*ter* 1 c.p.).

Il delitto di riciclaggio, così come formulato dall'art. 648- bis c.p., punisce chi ricicla denaro, beni o altre utilità provenienti da un delitto non colposo commesso da un altro soggetto, mentre nessuna sanzione era prevista per chi ricicla in prima persona , cioè sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo da egli commesso (o che ha concorso a commettere), ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. L'introduzione del reato di autoriciclaggio è stata necessaria per colmare questa lacuna nel nostro ordinamento. Il delitto di autoriciclaggio, peraltro, prevede pene diverse a seconda della gravità del delitto presupposto e con previsione della non punibilità delle condotte nelle quali il denaro, i beni o le altre utilità vengono destinati «alla mera utilizzazione o al godimento personale».

- **Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, introdotti dal D.Lgs. 184/2021 e modificato dalla L. n. 137/2023 (art. 25 octies I):**
  - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter, co. I c.p.).

Il delitto di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, così come formulato dall'art. 493 ter, co. I c.p., punisce chi indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti. La norma contempla, altresì, l'ipotesi del soggetto che falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. La novella del legislatore estende il campo della condotta, contemplando ogni strumento di pagamento diverso dal contante che sia idoneo ad abilitare al prelievo del denaro o all'acquisto di beni o prestazione di servizi o comunque rappresenti uno strumento di pagamento diverso dal contante.

  - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater, co. I c.p.).

La norma contempla l'ipotesi in cui, salvo che il fatto costituisca più grave reato, il soggetto che, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

- **Delitti di criminalità organizzata, introdotti dalla Legge 94/2009 (art. 24-*ter*):**

- Associazione per delinquere, anche diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-*bis*, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286 (art 416 c.p.).

I delitti associativi in generale hanno carattere plurisoggettivo, ossia richiedono la partecipazione di almeno tre persone. La partecipazione può essere anche di secondaria importanza, purché il contributo sia apprezzabile, concreto e dotato di effettiva stabilità.Ai fini della configurabilità del delitto di associazione per delinquere, è necessaria la predisposizione di un'organizzazione strutturale, sia pure minima, di uomini e mezzi, funzionale alla realizzazione di una serie indeterminata di delitti, nella consapevolezza, da parte dei singoli associati, di far parte di un sodalizio durevole e di essere disponibili ad operare per l'attuazione del programma criminoso comune. In altre parole, l'art. 416 c.p. punisce coloro che promuovono, costituiscono o organizzano l'associazione allo scopo di commettere più delitti. Anche il solo fatto di partecipare all'associazione costituisce reato. La rilevanza penale delle condotte descritte dalla norma appare condizionata all'effettiva costituzione dell'associazione criminosa. Infatti, prima ancora di richiamare le singole condotte di promozione, costituzione, direzione, organizzazione ovvero di semplice partecipazione, la norma ne subordina la punibilità al momento in cui «tre o più persone» si siano effettivamente associate per commettere più delitti. Il delitto di associazione per delinquere si caratterizza quindi per l'autonomia dell'incriminazione rispetto agli eventuali reati successivamente commessi in attuazione del *pactum sceleris*. Tali eventuali delitti, infatti, concorrono con quello di associazione per delinquere e, se non perpetrati, lasciano sussistere il delitto previsto dall'art. 416 c.p. Al netto delle considerazioni sopra svolte, la configurazione dei reati associativi come reati-mezzo ha l'effetto di estendere la responsabilità dell'ente ex decreto 231 a una serie indefinita di fattispecie criminose commesse in attuazione del *pactum sceleris* e non necessariamente incluse nell'elenco dei reati presupposto.

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25):**
  - Malversazione di erogazioni pubbliche (art. 316-*bis* c.p.);

Il reato di malversazione a danno dello Stato si perfeziona quando s'impiegano contributi, sovvenzioni, mutui agevolati o finanziamenti pubblici (statali, di altri enti pubblici o comunitari) ottenuti per la realizzazione di opere e attività di vario genere, per finalità diverse da quelle per le quali sono stati erogati. L'ipotesi criminosa si caratterizza per l'ottenimento di finanziamenti pubblici in modo lecito e per il successivo utilizzo degli stessi per finalità diverse da quelle sottese all'erogazione. Il delitto può essere commesso da chiunque, estraneo alla P.A. ometta di destinare, anche parzialmente, i fondi già ottenuti alle finalità per le quali gli stessi sono stati erogati. L'elemento soggettivo richiesto per l'integrazione della fattispecie è il dolo generico, sicchéè sufficiente la consapevolezza della provenienza dei fondi e la volontà di non impiegare gli stessi per le finalità per le quali erano stati concessi.

  - Indebita percezione di erogazioni pubbliche (art. 316-*ter* c.p.);

Il reato in esame si concretizza nell'indebito conseguimento, per sé o per altri, di fondi, comunque denominati, concessi o erogati dallo Stato, da altri Enti pubblici o dalle Comunità europee, mediante l'utilizzo o nella presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero nella omissione di informazioni dovute. A differenza della malversazione, dunque, la fattispecie in esame riguarda il conseguimento indebito dei finanziamenti, senza che a nulla rilevi l'uso che poi venga fatto delle erogazioni. In breve, mentre la malversazione integra le ipotesi d'indebito utilizzo di fondi regolarmente erogati e conseguiti, l'art. 316 ter punisce le attività connesse a un momento precedente, ossia quello di un'indebita percezione dei fondi.

  - Concussione (art. 317 c.p.);

Il reato di concussione si caratterizza per l'utilizzo indebito da parte del funzionario pubblico dei propri poteri, al fine di costringere il soggetto passivo a riconoscere al funzionario o ad un terzo soggetto un vantaggio di natura economica o personale. Si ha abuso dei poteri quando gli stessi siano esercitati fuori dei casi previsti da leggi, regolamenti e istruzioni di servizio o senza le forme prescritte, ovvero quando detti poteri, pur rientrando tra quelli attribuiti al pubblico ufficiale, vengano utilizzati per il raggiungimento di scopi illeciti.

- Truffa in danno dello Stato o di un ente pubblico (art. 640, comma 2, n. 1, c.p.);

L'ipotesi si configura nel caso in cui un qualunque soggetto, con artifici o raggiri tali da indurre in errore la controparte, procura a sè o ad altri un ingiusto profitto con danno dello Stato o di altro Ente pubblico. Trattasi di reato a dolo generico, sicché per la consumazione dello stesso è necessario che ricorrano tanto il profitto per il privato quanto il danno per lo Stato; l'assenza di tali elementi determina la necessaria qualificazione delle condotte fraudolente come ipotesi di truffa tentata e non consumata.

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

La fattispecie in oggetto consta dei medesimi elementi costitutivi della truffa semplice (art. 640 c.p.) ma rappresenta più grave ed autonoma fattispecie in quanto l'ingiusto profitto per il privato è rappresentato da contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri Enti pubblici o delle Comunità europee. Tale ipotesi si distingue dunque da quella prevista e punita ex art. 640, co. 2 n. 1 c.p. per la diversa natura del profitto, mentre si distingue dall'ipotesi di cui all'art. 316 ter c.p. per le diverse e più gravi modalità della condotta, che nella fattispecie in esame risulta più marcatamente connotata da comportamenti fraudolenti. Con la sentenza n. 5150/2013, la Corte di Cassazione ha affermato che in caso di procedimento "231" a seguito di truffa ai danni dello Stato per il conseguimento di pubbliche erogazioni, è legittimo il sequestro operato in capo al soggetto che, pur non essendo il diretto richiedente dell'erogazione, ne risulta il destinatario finale, in virtù di un rapporto a carattere privato con il ricevente principale. Segnatamente, il finanziamento pubblico era stato ricevuto da un soggetto privato che, mediante la sottoscrizione di contratti di appalto, lo ha a sua volta corrisposto alla società in questione. Tuttavia, secondo la Suprema Corte, la presenza di un "intermediario" non sarebbe sufficiente a far venir meno il carattere pubblico della somma di denaro.

- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.);

L'intervento manipolativo può essere tale da modificare gli scopi cui il sistema informatico è destinato, ma il reato ricorre anche quando - pur nel rispetto della destinazione del sistema - sono manipolati i contenuti dello stesso. Diversamente, la condotta alternativa di 'intervento abusivo' è rivolta ai dati, alle informazioni (cioè, per semplificare, ad un insieme di dati) o ai programmi (software) installati nell'hardware. In particolare, va rilevato che l'intervento, per configurare la condotta descritta dalla fattispecie ex art. 640 ter c.p., deve avvenire "senza diritto" e, dunque, non solo in assenza del necessario consenso del titolare dei dati, informazioni e programmi contenuti nel sistema informatico, ma anche secondo una modalità non consentita da norme giuridiche, né da altre fonti. Il reato di frode informatica presenta, in breve, la medesima struttura e i medesimi elementi costitutivi del reato di truffa da cui si distingue in quanto l'attività illecita investe non la persona ma un sistema informatico. Nel reato di frode informatica, pertanto, non assume rilevanza - a differenza che nel reato di truffa - il ricorso da parte dell'autore del reato ad artifizi o raggiri, ma l'elemento oggettivo dell'alterazione del sistema informatico (e/o dei dati in esso disponibili).

- Corruzione (artt. 318, 319, 320, 322-*bis* c.p.);

Il reato di corruzione consiste in un accordo fra un pubblico funzionario e un privato, in forza del quale il primo accetta dal secondo un compenso che non gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria). Nella corruzione il pubblico ufficiale ed il privato sono in posizione paritaria, diversamente dalla concussione che invece presuppone lo sfruttamento da parte del funzionario della propria posizione di superiorità alla quale corrisponde una situazione di soggezione nel privato. La fattispecie prevista dall'art. 319 c.p., connotata come quella di cui all'art. 318 c.p. da un rapporto paritetico tra pubblico ufficiale/ incaricato di un pubblico servizio-corrotto e privato-corruttore, se ne differenzia in virtù del fatto che l'atto richiesto al pubblico ufficiale o all'incaricato di un pubblico servizio a fronte della dazione o della promessa di denaro o di altra utilità, risulta contrario ai doveri d'ufficio. In particolare la condotta può concretizzarsi in una omissione o in un ritardo nel compimento di un atto di ufficio ovvero nel compimento di un atto contrario ai doveri di ufficio.

- Istigazione alla corruzione (art. 322 c.p.);

Il reato è configurabile solo ove l'offerta del privato o la richiesta del pubblico funzionario non vengano accolte dal destinatario. Tuttavia, ove il rifiuto non sia stato immediato e siano incorse trattative poi non sfociate in un accordo, si ritiene configurabile un tentativo di corruzione del quale rispondono entrambi i soggetti. Nell'istigazione alla corruzione passiva la condotta consiste nell'offrire o nel promettere denaro o altra utilità non dovuti al funzionario. L'offerta o la promessa deve essere seria e concreta ed idonea alla realizzazione dello scopo, tale cioè da indurre il destinatario a compiere o a ritardare un atto dell'ufficio o del servizio ovvero a fare un atto contrario a detti doveri. L'idoneità dell'offerta va valutata con un giudizio "ex ante" che tenga conto dell'entità del compenso, delle qualità personali del destinatario e della sua posizione economica e di ogni altra connotazione del caso concreto.

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

Per quanto riguarda il reato di corruzione in atti giudiziari (art. 319 ter c.p.), si precisa che tale fattispecie non ricorre soltanto in relazione all'esercizio delle funzioni giudiziarie cui è subordinata e allo status di colui che le esercita, ma ha una portata più ampia. Infatti, come precisato dalla Corte di Cassazione, costituisce "atto giudiziario" qualsiasi atto funzionale a un procedimento giudiziario, indipendentemente dalla qualifica soggettiva di chi lo realizza (cfr. Cass., Sezioni Unite, sentenza n. 15.208 del 25/2/2010, con riferimento alla testimonianza resa in un processo penale).

- Corruzione tra privati (art. 2635 c.c.);

La nuova formulazione dell'art. 2635 c.c. estende il novero dei soggetti attivi includendo tra gli autori del reato, oltre a coloro che rivestono posizioni apicali di amministrazione o di controllo, anche coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive presso società o enti privati. Ai fini "231", per quanto concerne la corruzione tra privati, resta reato-presupposto la sola fattispecie di cui al comma 3 dell'articolo 2635 del codice civile, cioè il delitto commesso da chi corrompe, oggi anche per interposta persona, i soggetti indicati nel primo comma del medesimo articolo (nella sua nuova e più estesa versione) per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

- Istigazione alla corruzione tra privati (art. 2635 *bis* c.c.)

Diventa invece nuovo reato-presupposto anche l'istigazione alla corruzione tra privati (nuovo articolo 2635-bis comma 1). Anche in questo caso solo a carico della società alla quale appartiene il soggetto che istiga alla corruzione gli esponenti aziendali altrui, per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

- Frode nelle pubbliche forniture (art. 356 c.p.);

Tale fattispecie punisce chiunque commette frode nell'esecuzione dei contratti di fornitura conclusi con lo Sato, con un Ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità. Per giurisprudenza e dottrina costante è richiesto un inadempimento dell'obbligazione parziale o inesatto ma anche in un adempimento totale. La condotta consiste nella frode nel corso dell'esecuzione di uno dei contratti indicati nell'art. 255 e pertanto devono riguardare cose od opere necessarie a unostabilimento pubblico o a un pubblico servizio.

- Peculato (art. 314, co. 1, c.p.);

Il reato si configura quando un pubblico ufficiale o un incaricato di un pubblico servizio si appropria di denaro o di altra cosa mobile altrui, di cui lo stesso è in possesso per ragione del suo ufficio o servizio. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

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

Il reato punisce il pubblico ufficiale o l'incaricato di un pubblico servizio, che, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

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

Tale reato punisce, salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

La fattispecie potrebbe realizzarsi, in concreto, nel caso in cui un dipendente dell'impresa, approfittando di rapporti personali con il funzionario pubblico preposto al rilascio di determinati permessi e/o autorizzazioni, prenda contatto con quest'ultimo per ottenere un provvedimento favorevole nell'interesse dell'impresa, pur consapevole di non averne diritto. Il dipendente (e con lui l'impresa nel cui interesse lo stesso abbia agito) risponderebbe a titolo di concorso dell'extraneus nel reato "proprio".

- **Reati contro la personalità individuale, introdotti dalla legge 228/2003, e modificati con la legge 38/2006, e dalla legge 199/2016 (art. 25-*quinquies*):**

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)

La norma descrive due ipotesi delittuose. La prima riconduce alla nozione di "schiavitù" "l'esercizio su una persona di poteri corrispondenti a quelli del diritto di proprietà". Quindi sono compresi sia le tipiche facoltà inerente al diritto di proprietà, cioè godere e disporre, sia l'esercizio di diritti reali minori. Invece la seconda figura prescinde dal richiamo al diritto domenicale e si distingue due momenti: lo sfruttamento coattivo di una persona e la condizione di assoggettamento dall'altro. La sinergia tra queste due condizioni permette di individuare il reato de quo quando la persona diventa una "cosa" poiché la sua vita è interamente determinata a sistematicamente finalizzata per la realizzazione di utilità godute da soggetti terzi. *Ex* D.lgs. 231/2001, la condotta rilevante in questi casi è costituita dal procacciamento illegale della forza lavoro attraverso il traffico di migranti e la tratta degli schiavi.

- Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.)

Il reato in esame, oggi, risulta slegato dal requisito dello svolgimento di «*un'attività organizzata di intermediazione*», andando a colpire non solo chi «*recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento...*», ma altresì chiunque «*utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno*». Anche gli "indici di sfruttamento" enunciati dall'art. 603-*bis* c.p. assumono una connotazione più ampia, essendo oggi alcuni di essi parametrati, ad esempio, non più a condotte sistematiche di sotto retribuzione e violazione delle norme su orari, riposi, aspettativa e ferie, bensì a siffatte condotte anche solo «reiterate». La punibilità dell'enteè dunque collegata al compimento di un reato non più limitato a chi svolge attività organizzata d'intermediazione, né legato a violenza e minaccia come elementi costitutivi. Reato connotato inoltre da «uno sfruttamento» la cui presenza è dedotta dalla semplice reiterazione di condotte di retribuzione palesemente difforme dai contratti collettivi nazionali o territoriali, dalla violazione delle norme su orario, riposo, aspettativa e ferie o dalla mera sussistenza di violazione delle norme antinfortunistiche, anche non tali da esporre a pericolo il lavoratore. A contemperamento di una siffatta estensione nella possibile applicazione della norma, si deve tuttavia considerare la natura dolosa del reato in esame, con la conseguenza che le condotte costituenti "indice di sfruttamento" rileveranno solo ove dolosamente preordinate a sottoporre «i lavoratori a condizioni di sfruttamento» con consapevolezza e volontà di approfittare «del loro stato di bisogno».

➢ Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies*)

Ai sensi dell'art. 25-*duodecies*, comma 1-*bis*, la condotta tipica è quella di colui il quale ("chiunque") promuova, diriga, organizzi, finanzi o effettui il trasporto di stranieri nel territorio dello Stato ovvero compia altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di un altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente e nel caso in cui: il fatto riguardi l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone; la persona trasportata sia stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale; la persona trasportata sia stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale; il fatto sia commesso da tre o più persone in concorso fra loro utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti; gli autori del fatto abbiano la disponibilità di armi o materie esplodenti. L'art. 25-duodecies, comma 1-*ter*, prevede invece il caso in cui un soggetto, agendo nell'interesse o a vantaggio della società, al fine di trarre un ingiusto profitto dalla condizione d'illegalità dello straniero o nell'ambito delle attività punite a norma dell'art. 12 D.Lgs. 286/1998, favorisca la permanenza dello straniero nel territorio dello Stato in violazione delle norme del Testo Unico sull'immigrazione.

➢ Reati tributari, introdotti dalla L. n. 157/2019 (art. 25-*quinquiesdecies*):

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. n. 74/2000)

L'art. 2 del D.lgs 74/2000 prevede che sia punito chiunque al fine di evadere le imposte sui redditi e l'Iva indica in una dichiarazione elementi passivi fittizi attraverso fatture o altri documenti per operazioni inesistenti. Seconda consolidata giurisprudenza, integra il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, la falsa indicazione, nella dichiarazione Irpef, di spese deducibili dall'imposta, quando le stesse non siano state effettuate o siano state effettuate in misura inferiore. (cfr.Cass. civ., n. 48486/2011 e 27392/2012). In relazione al mezzo fraudolento di cui l'agente si avvale per l'indicazione in dichiarazione di elementi passivi fittizi, la Corte di cassazione ha fornito, una definizione degli altri documenti rilevanti ai sensi dell'art. 2 del d.lgs. n. 74/2000, precisando che tali sono quelli «[…] aventi, ai fini fiscali, valore probatorio analogo alle fatture (documenti tipici fiscali previsti espressamente dal d.P.R. 633/1972, art. 21)». Pertanto, può dirsi che ai fini della sussistenza del reato di dichiarazione fraudolenta di cui all'art. 2 del d.lgs. 74/2000, per fatture o altri documenti per operazioni inesistenti devono intendersi quelli che, a prescindere dal *nomen*, hanno l'attitudine, in base alle norme dell'ordinamento tributario, a fornire la prova delle operazioni in essi documentati. A tal fine non è necessario stabilire *ex post* se il documento possa avere tale attitudine ma è sufficiente che, per le sue caratteristiche estrinseche e per il suo contenuto, tale natura non possa essere esclusa *ictu oculi* in base alle norme dell'ordinamento tributario sin dalla fase dell'accertamento fiscale (Cassazione penale sez. III, 27/02/2018, n.40448).

- Dichiarazione fraudolenta mediante altri artifici (art.3 D.lgs n. 74/2000)

La dichiarazione fraudolenta potrà essere realizzata, oltre che con le modalità previste dall'articolo precedente, anche con l'utilizzo di altri artifizi. Quest'ultima è costruita, essenzialmente, come frode contabile, alla quale deve associarsi un *quid pluris* artificioso non tipizzato (diverso dall'uso di fatture o altri documenti falsi, integrante l'ipotesi di cui al precedente art. 2) ma, comunque, caratterizzato dall'idoneità a indurre in errore e a impedire il corretto accertamento della realtà contabile del soggetto che presenta la dichiarazione annuale d'imposta, come:la tenuta di un sistema parallelo di contabilità "nera"; la vendita "a nero" organizzata in locali contigui a quelli aziendali; la voluta "confusione" di ricavi provenienti da fonti diverse in modo da impedire di individuare il titolare degli stessi; lo spostamento artificioso di redditi tra soggetti rivolto a fare figurare come percepiti da terzi redditi propri del contribuente.

- Dichiarazione infedele (art. 4 D. Lgs. n. 74/2000)

Fuori dei casi previsti dagli articoli 2 e 3, è punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.
La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).

- Omessa dichiarazione (art. 5 D.lgs. n. 74/2000)

È punito chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila. **La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).**

- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs n. 74/2000)

L'art. 8 del D.lgs n. 74/2000 punisce chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.La realizzazione della condotta *de qua* necessita che la fattura o il documento escano dalla sfera di fatto e di diritto dell'emittente mediante consegna o spedizione a un terzo potenziale utilizzatore, che non abbia partecipato alla perpetrazione del falso. La condotta delittuosa in esame, si pone all'inizio di un percorso che porterà, nella maggior parte dei casi, all'utilizzo di tali documenti e quindi al concretizzarsi del reato di cui all'art. 2 – dichiarazione fraudolenta - realizzando appieno quel *fine di consentire a terzi l'evasione*. Sono reati legati dall'unicità del fine, nel senso che il primo (art. 8) costituisce il mezzo normale per realizzare il secondo (art. 2).

- Indebita compensazione (art. 10 *quater* D. Lgs. n. 74/2000)

È punito chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro. È punito chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro. **La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).**

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

5. REGOLE GENERALI DI COMPORTAMENTO

Coerentemente con i princìpi deontologici aziendali di cui al Codice Etico del Gruppo Battistolli, il personale della Società deve far riferimento ai seguenti principi di comportamento:

- lealtà, correttezza, trasparenza, competenza, professionalità, criteri di concorrenza ed economicità nella scelta dei fornitori/professionisti e nella gestione dei rapporti con gli stessi;
- principio di equità nell'erogazione di tutti i compensi e/o somme corrisposte per forniture/incarichi professionali, sulla base di valutazioni obiettive e imparziali, nonché l'adeguata tracciabilità della documentazione relativa alle offerte;
- imparzialità nella selezione dei fornitori/professionisti e nella determinazione delle condizioni d'acquisto di beni e servizi, affinché avvengano sulla base di valutazioni obiettive, fondate sulla qualità, sul prezzo e sulle garanzie fornite.

Coerentemente è fatto divieto di:

- effettuare prestazioni o pagamenti in favore di collaboratori, fornitori, consulenti, *partner* o altri soggetti terzi che operino per conto della Società e che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e al tipo di incarico da svolgere;
- effettuare pagamenti attraverso cessioni del credito, qualora tale modalità non sia formalmente prevista e autorizzata all'interno dell'accordo stipulato con il fornitore o *partner* commerciale;
- attivare consulenze senza garantire congruità, adeguatezza e documentabilità dell'iniziativa;

- favorire ingiustificatamente nei processi di acquisto collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da rappresentanti della Pubblica Amministrazione;
- utilizzare il processo d'acquisto di beni e servizi per influenzare la volontà o l'indipendenza di giudizio di rappresentanti della Pubblica Amministrazione al fine di ottenere ingiustificati vantaggi o evitare la comminazione di sanzioni;
- favorire fornitori scelti principalmente in base a criteri di amicizia, parentela o qualsiasi altra cointeressenza tale da inficiarne la validità in termini di prezzo e/o qualità ovvero che risultino strumentali alla realizzazione di una delle condotte illecite indicate nel D.lgs. n. 231/2001;
- fare un utilizzo improprio degli strumenti di pagamento diversi dal contante;
- alterare, distrarre o mettere a disposizione d'altri gli strumenti di pagamento diversi dal contante;
- alterare i sistemi informatici al fine di modificare o alterare strumenti di pagamento diversi dal contante.

Chiunque venga a conoscenza di tali ipotesi è tenuto a segnalarle direttamente all'Organismo di Vigilanza.

Sono altresì vietate condotte volte a esercitare pressioni nei confronti delle Funzioni coinvolte nelle attività oggetto del protocollo (anche basate sul grado o sulla funzione ricoperta all'interno dell'Azienda) al fine di eludere le presenti disposizioni. È fatto obbligo di segnalare all'Organismo di Vigilanza, anche senza riferimenti a nominativi, l'eventuale esistenza di tali condotte o l'instaurarsi di prassi di questo genere.

La Società condanna tramite l'applicazione del Sistema Disciplinare i comportamenti difformi ai princìpi sopra menzionati, nonché ai presidi di controllo di seguito riportati.

I contratti con collaboratori, fornitori, consulenti/professionisti, *partner* o altri soggetti terzi che operino per conto della Società dovranno, contenere:

- informativa sulle norme comportamentali adottate e definite all'interno del Codice Etico, nonché sulle conseguenze che comportamenti contrari allo stesso e alle normative vigenti possono avere con riguardo ai rapporti contrattuali;
- dichiarazione di conoscenza della normativa di cui al D.lgs. 231/01 e di impegno al suo rispetto (ovvero, se si tratta di soggetto straniero o operante all'estero, dichiarazione di conoscenza e impegno al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti alla corruzione e alla truffa ai danni di Enti Pubblici);
- laddove il professionista/consulente sia dipendente o collabori con Enti Pubblici, dichiarazione di assolvimento degli adempimenti eventualmente richiesti dall'Ente stesso per l'assunzione dell'incarico (se applicabile).

6. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee guida di Confindustria, nonché delle "*best practice*", prevede con riferimento alle Aree e alle

Attività Sensibili individuate:

- *standard di controllo generali*", applicabili a tutte le Attività Sensibili;
- *standard di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

6.1 STANDARD DI CONTROLLO "GENERALI"

I presidi di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:

- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;
- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa. Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

6.2 STANDARD DI CONTROLLO SPECIFICI

Sulla base dei presidi di controllo generali sopra riportati, i presidi di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole

di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;
- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema delle deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

7. GESTIONE DELLE FORNITURE DI BENI E SERVIZI

7.1. SELEZIONE DEI FORNITORI DI BENI E SERVIZI

Per poter essere fornitore del Gruppo Battistolli è necessario concludere positivamente il processo di accreditamento finalizzato alla valutazione di molteplici dimensioni, dalle capacità tecniche e gestionali, all'affidabilità etica, economica e finanziaria. Tale processo permette al Gruppo Battistolli di avere un'approfondita conoscenza dei propri fornitori attraverso uno strumento innovativo e altamente efficace per la selezione, in coerenza con quanto previsto dalla normativa vigente, all'interno di un ciclo virtuoso finalizzato al reciproco miglioramento e al raggiungimento degli obiettivi prefissati.

Il processo di qualifica del fornitore ha inizio con la registrazione in apposito elenco suddiviso per categoria merceologica, che identifica gli operatori economici. I fornitori il cui processo di qualifica ha avuto esito positivo sono evidenziati in verde. In giallo vengono evidenziati quelli che non hanno prodotto tutta la documentazione e che vengono sollecitati al fine di confermarne la qualifica. In rosso quelli che presentano criticità e per i quali viene sospesa qualsiasi attività fino a eventuale riscontro positivo.

Tra i fornitori catalogati non sono inclusi quelli che forniscono utilities (come i servizi telefonici, elettricità o altro). Per i fornitori relativi agli specifici Uffici (Network, Legale, Risorse Umane, Sistemi Informativi, Ufficio Sicurezza, Ufficio Immagine, Sponsorizzazioni, Comunicazione, dell'Assistenza Tecnica Commerciale Rangers, Sistemi Informativi, Ufficio Sicurezza) il processo di accreditamento viene effettuato in collaborazione tra la Ufficio Acquisti e la Funzione coinvolta. Le Funzioni interessate dovranno coinvolgere, preventivamente all'acquisto, l'Ufficio Acquisti per

un'analisi dell'affidabilità del fornitore. L'Ufficio Acquisti verificherà il corretto inserimento del fornitore e contestualmente assegnerà la qualifica con il relativo rating.

La procedura è sviluppata per migliorare l'efficienza dei processi di acquisto e apportare importanti benefici anche agli operatori economici in termini di:

- trasparenza e concorrenzialità;
- snellimento e dematerializzazione del processo negoziale;
- rispetto dei requisiti di riservatezza, autenticità e integrità nello scambio dei dati;
- garanzia di affidabilità e sicurezza;
  sostenibilità ambientale.

Questo procedimento permette ai fornitori di inserire i propri dati aziendali e sottoscrivere i documenti del Gruppo. In questa fase ai fornitori viene chiesto di compilare dei questionari per verificarne le credenziali. Allo scopo di indurre nei fornitori l'adozione di comportamenti socialmente responsabili ed ecosostenibili, nel processo di selezione sono considerati preferenziali la presenza di certificazioni o politiche sociali e ambientali. Le informazioni richieste possono essere supportate da idonea documentazione.

La documentazione richiesta in fase di registrazione è elencata nell'Appendice 2 della policy acquisti, cui si rinvia.

L'esito positivo del processo di accreditamento comporta l'inserimento del fornitore nell'Elenco dei Fornitori Qualificati del Gruppo Battistolli per la categoria merceologica oggetto del processo.

La qualificazione di una impresa in un determinato comparto merceologico ha lo scopo di assicurare che il potenziale titolare di un contratto possieda caratteristiche idonee dal punto di vista legale, si trovi in una situazione economico-finanziaria soddisfacente, abbia una potenzialità produttiva adeguata alle caratteristiche della tipologia di fornitura o servizio per la quale viene qualificato e sia in grado di fare fronte agli *standard* fissati dal Gruppo Battistolli per la suddetta tipologia, dal punto di vista sia delle capacità tecnico/professionali, sia dell'adeguatezza del sistema qualità aziendale, nei casi in cui lo stesso è richiesto.

Qualora l'Ufficio Acquisti, durante il processo di approvvigionamento, non riscontrasse la presenza di alcun fornitore idoneo tra quelli accreditati, procede a individuare nuovi fornitori attraverso indagini di mercato.

La necessità di qualificare nuovi fornitori può nascere dal fatto che tra i fornitori qualificati non ci sia chi possa essere in grado di soddisfare la data di consegna richiesta, di fornire il prodotto cercato, di offrire le garanzie richieste o significativi vantaggi commerciali.

I nuovi fornitori individuati sono invitati a superare la fase di accreditamento, salvo che non si tratti di acquisti spot per importi fino a un massimo di euro 5.000,00. Nel caso in cui, nel corso dell'anno, tali acquisti dovessero ripetersi, il fornitore sarà invitato a registrarsi.

In caso di urgenza effettiva, dichiarata dai Direttori di Divisione e/o Amministratori Delegati competenti e/o Responsabili di Funzione, per acquisti fino ad un massimo di euro 25.000,00 il Fornitore dovrà accreditarsi prima possibile e comunque non oltre 15 (quindici) giorni dalla richiesta.

L'accreditamento costituisce condizione per poter partecipare ad eventuale gara indetta per la scelta del Fornitore. Le registrazioni dei risultati delle valutazioni e di tutte le azioni necessarie scaturite dalla valutazione devono essere conservate.

Nel caso in cui il fornitore, per l'erogazione di un servizio o parti di esso, si avvalga di strutture terze con le quali formalizza rapporti contrattuali specifici, e comunque avallati preventivamente dalle Società del Gruppo, il subappaltatore dovrà essere sottoposto a idonea verifica in ordine al possesso dei requisiti che siano quantomeno omologhi a quelli del fornitore qualificato, laddove il valore del servizio affidato al terzo ecceda il 50%. In ogni caso il soggetto che si avvale della struttura terza deve garantire che lo stesso sia in possesso dei requisiti stabiliti dalla presente Procedura, relativamente al servizio prestato, attraverso certificazione di terza parte, oppure verifica diretta da parte del fornitore stesso.

Il fornitore registrato può in qualsiasi momento chiedere di modificare e/o aggiornare i dati di iscrizione e le classificazioni merceologiche selezionate. La modifica dei dati comporta una nuova valutazione dell'idoneità del fornitore e un nuovo processo di accreditamento.

L'iscrizione all'Elenco Fornitori Qualificati potrà essere revocata in caso di eventi tali da modificare il quadro di riferimento preso in considerazione all'atto dell'iscrizione:

- ristrutturazione aziendale;
- gravi difficoltà economiche-finanziarie;
- situazioni di contenzioso;
- in caso di grave inadempimento degli obblighi contrattuali relativamente a contratti in corso di esecuzione;
- qualsiasi altro grave evento che comprometta il rapporto fiduciario;
- per non aver risposto per tre volte consecutive all'invito a presentare offerta;
- violazione del Codice Etico del Gruppo Battistolli;
- per non conferma del fornitore a seguito del monitoraggio della presente procedura, come di seguito indicato.

All'atto della contrattualizzazione dei rapporti con il fornitore, il contratto sottoscritto deve necessariamente contenere la seguente clausola generale:

"Il fornitore dichiara di conoscere le prescrizioni contenute nel Codice Etico adottato da Rangers S.r.l. e nel Modello di Organizzazione, gestione e controllo ex D.lgs. 231/01, e dichiara, inoltre, di accettarle integralmente, astenendosi da comportamenti a esse contrari. L'eventuale inosservanza di tali princìpi potrà costituire inadempimento contrattuale, legittimando Rangers S.r.l. a risolvere il presente contratto ai sensi e per gli effetti dell'articolo 1456 del Codice Civile, fermo restando il diritto al risarcimento dei danni eventualmente subiti dalla Società per effetto di detto inadempimento."

Il rispetto dei requisiti richiesti ai fornitori è garantito tramite adeguate procedure di monitoraggio che tengono conto anche dei profili di rischio delle diverse categorie di fornitori.

L'Elenco Fornitori Qualificati dovrà essere periodicamente aggiornato dal Responsabile dell'Ufficio Acquisti e la documentazione dovrà essere aggiornata con cadenza almeno annuale e comunque ogniqualvolta si evidenzino variazioni significative rispetto alla struttura interna del Fornitore stesso o in caso di situazioni che possano incidere sulla sua affidabilità. Il Responsabile Gestione Qualità riporta eventuali elementi conoscitivi che si verificassero nel tempo quali, a titolo esemplificativo, materiali non conformi o ritardi nelle consegne.

Con cadenza annuale viene eseguito un monitoraggio dei fornitori attivi con fatturato superiore a € 25.000,00 inseriti registrando tutte le eventuali segnalazioni di non conformità.

L'Organismo di Vigilanza verifica la corretta applicazione delle procedure.

7.2 PROCESSO DI APPROVVIGIONAMENTO DI BENI E SERVIZI

La gestione di acquisti di beni e servizi deve avvenire secondo il principio generale di buona fede e con la diligenza ordinaria nella gestione delle attività, nel rispetto dei princìpi espressi dal Codice Etico e in applicazione della Procedura Aziendale 2.3 e delle altre procedure operative, che vengono qui integralmente richiamate per quanto di competenza.

La procedura adottata dalla Società relativa alla gestione dei rapporti con i fornitori prevede tra l'altro: (a) la coerenza tra le richieste di acquisto e i relativi ordini di acquisto; (b) la segregazione delle funzioni tra chi richiede, chi dispone e chi autorizza un acquisto, una fornitura o comunque una spesa; (c) le informazioni di carattere generale e specifico che consentano di individuare in modo esauriente e non ambiguo l'acquisto/fornitura e le modalità di erogazione dello stesso; (d) il contenuto minimo di qualsiasi richiesta e ordine di acquisto.

Il processo di acquisto ha inizio con la compilazione della Richiesta di Approvvigionamento. Quest'ultima è il documento in formato elettronico a uso interno che deve essere compilato a cura del Richiedente, come previsto dal Sistema Qualità ISO 9001:2015, completo di ogni dettaglio e allegato, e in particolar modo:

- nome del richiedente;
- motivazioni per cui si richiede l'acquisto;
- dati di eventuali fornitori suggeriti e motivazione della scelta;
- descrizione dettagliata dei beni da acquisire, quantità e indicazione della spesa presunta;
- eventuali campioni o bozze;
- data della richiesta.

Per Richiedente si intende:

- il Responsabile di Filiale/Reparto/Settore/Addetto/Referente area conta;
- ogni altra Funzione competente gerarchicamente superiore rispetto alle precedenti.

La Richiesta di Approvvigionamento deve poi essere inoltrata, sempre a cura del Richiedente, al Responsabile di Filiale/Sede/Coordinatore/Referenti area conta che deve:

- verificarne l'effettiva necessità;
- verificarne la corretta compilazione;
- restituirla al Richiedente per le eventuali spiegazioni/integrazioni;
- autorizzare tramite piattaforma informatica per conferma dopo gli opportuni controlli.

Se il Responsabile di Filiale/Sede/Coordinatore approva nell'applicativo dedicato la Richiesta di Approvvigionamento, la stessa seguirà il *workflow* previsto dalla Policy approvvigionamenti, dopo le opportune verifiche ed eventuali integrazioni. Il Risk&Regional Security Manager sarà informato e per conoscenza qualora l'acquisto sia inerente alla sicurezza ovvero uno degli ambiti presidiati.

Gli Uffici competenti provvedono alla valutazione e selezione del fornitore, a seconda delle caratteristiche della richiesta, utilizzando i fornitori accreditati secondo quanto specificato nell'Appendice 3 della Policy approvvigionamenti ("Criteri di scelta dei fornitori per casi definiti").

Per tutti gli altri casi, ricevuta la Richiesta di Approvvigionamento, gli Uffici competenti, al fine di ottenere, a parità di qualità del bene/servizio, le migliori condizioni economiche, e tenendo conto di eventuali suggerimenti da parte della Funzione Richiedente, inviano la richiesta di offerta:

- **Per forniture fino a 1.500 euro, il controllo deve avvenire con almeno una di queste condizioni**:
  - Un preventivo
  - Ricerca internet per verifica prezzi
  - Comparazione con ordini simili

- **Per forniture da 1.500 a 10.000 il controllo deve avvenire con almeno tre di queste condizioni**:
  - Un preventivo obbligatorio
  - Ricerca internet per verifica prezzi
  - Comparazione con ordini simili
  - Richiesta di almeno un altro preventivo anche via web

- **Per forniture oltre a € 10.000,00 e fino a € 50.000,00 il controllo deve avvenire con almeno tre di queste condizioni**:
  - Due preventivi obbligatori
  - Richiesta di un altro preventivo anche via web
  - Ricerca internet per verifica prezzi
  - Comparazione con ordini simili

- **Per forniture oltre a € 50.000,00 e fino a € 150.000,00 il controllo deve avvenire con almeno quattro di queste condizioni**:
  - Tre preventivi obbligatori

- Richiesta di un altro preventivo anche via web
- Ricerca internet per verifica prezzi
- apertura mini contest
- verbale contenente le autorizzazioni delle funzioni coinvolte

➢ **Per progetti specifici e/o forniture oltre a € 150.000,00**, in aggiunta a quanto previsto dal punto precedente, il processo autorizzativo deve obbligatoriamente essere corredato di un verbale di tutte le funzioni coinvolte che definisca i termini e le condizioni del progetto.

Il sistema informativo aziendale prevede un iter autorizzativo per il rilascio degli Ordini di Acquisto. L'Ordine di Acquisto è giuridicamente valido dal momento in cui il soggetto preposto all'autorizzazione di spesa sottoscrive il documento. Di seguito, si riportano i workflow autorizzativi.

WORKFLOW AUTORIZZATIVI

Il workflow autorizzativo prevede, per gli Uffici Corporate o con disciplina condivisa:

➢ **REPARTO IT**

- Le richieste da € 0 a € 5.000,00 sono inserite e approvate direttamente dal Responsabile IT e in c.c. al Direttore di Funzione;
- le richieste oltre € 5.000,00 sono inserite e approvate direttamente dal Responsabile IT e dall'AD di riferimento e in c.c. al Direttore di Funzione.

Si specifica che tutti gli acquisti riguardanti software, licenze, hardware e dispositivi IOT in generale, da collegare in rete dati aziendale, dovranno essere preventivamente condivisi con i Sistemi Informativi. Per quanto concerne le dotazioni IT è prevista l'assegnazione in base al cluster di appartenenza. In caso di mutamento e/o cessazione le dotazioni dovranno essere restituite per essere riutilizzate (libere da eventuali codici di blocco e/o documenti, files etc., in pratica riportato alle condizioni di fabbrica). Non sono previste doppie dotazioni, quindi la fornitura di un notebook, a discrezione del Direttore di Funzione/Divisione, sostituisce la postazione fissa. Eventuali eccezioni dovranno essere preventivamente autorizzate dall'AD di riferimento.

➢ **GARE / ACQUISTI / AUTOMEZZI**

- Le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile di Funzione e in c.c. al Direttore di Funzione e all'AD di riferimento;
- le richieste oltre € 1.001,00 e fino a € 5.000 devono essere approvate dal Direttore di Funzione e in c.c. all'AD di riferimento;
- le richieste oltre € 5.000 devono essere approvate dal Direttore di Funzione e dall'AD di riferimento.

➢ **AMMINISTRAZIONE / LEGALE**

- Le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile di Funzione e in c.c. al Direttore di Funzione e all'AD di riferimento;

- le richieste oltre € 1.001,00 e fino a € 5.000 devono essere approvate dal Direttore di Funzione e in c.c. all'AD di riferimento;
- le richieste oltre € 5.000 devono essere approvate dal Direttore di Funzione e dall'AD di riferimento.

➢ **HR**
- Le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile di Funzione e in c.c. al Direttore di Funzione e all'AD di riferimento;
- le richieste oltre € 1.001,00 e fino a € 5.000 devono essere approvate dal Direttore di Funzione e in c.c. all'AD di riferimento;
- le richieste oltre € 5.000 devono essere approvate dal Direttore di Funzione e dall'AD di riferimento.

➢ **FATTURAZIONE**
- le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile dell'Ufficio e in c.c. al Responsabile di Funzione;
- le richieste oltre € 1.001,00 e fino a € 5.000 devono essere approvate dal Responsabile di Funzione e in c.c. all'AD di riferimento;
- le richieste oltre € 5.000 devono essere approvate dal Responsabile di Funzione e dall'AD di riferimento.

➢ **NETWORK**
- le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile dell'Ufficio e in c.c. al Responsabile di Funzione;
- le richieste oltre € 1.001,00 e fino a € 5.000 devono essere approvate dal Responsabile di Funzione e in c.c. all'AD di riferimento;
- le richieste oltre € 5.000 devono essere approvate dal Responsabile di Funzione e dall'AD di riferimento.

➢ **IMMAGINE**
- le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile dell'Ufficio e in c.c. al Direttore di Funzione e all'AD di riferimento;
- le richieste oltre € 1.000,00 devono essere approvate dal Direttore di Funzione e dall'AD di riferimento.

➢ **COMUNICAZIONE**
- le richieste da € 0 a € 1.000,00 sono inserite e approvate direttamente dal Responsabile di Funzione e in c.c. all'AD di riferimento;
- le richieste oltre € 1.000,00 devono essere approvate dall'AD di riferimento.

➢ **SICUREZZA SUL LAVORO – D.LGS. 81/08 DATORE DI LAVORO O DELEGATO DEL DATORE DI LAVORO; FORMAZIONE**

Le richieste sono inserite dal Manager HSE o dal Responsabile di filiale/Reparto e validate dal Manager HSE e approvate direttamente dal DL o DDL e in c.c. all'AD.

Per gli approvvigionamenti previsti dal D.lgs. 81/2008 gli RSPP provvedono a indicarne la necessità nei DVR, documenti equipollenti o relazioni specifiche. Nel caso la stessa sia inserita dal Responsabile di Filiale/Reparto o da altra figura che ne abbia i poteri, il Manager HSE dovrà

approvare quanto contenuto o modificarlo se necessario e solo successivamente andrà al Datore di Lavoro o al suo Delegato che dovrà approvarne l'acquisto dando priorità a tutte le richieste che riguardano in generale la sicurezza di lavoratori e dipendenti, mettendo sempre in copia l'AD.
Per quanto riguarda le spese legate alla formazione, la richiesta dovrà essere inserita dal Responsabile di filiale/Reparto o da altra figura che ne abbia i poteri e dovrà essere approvata dal Responsabile dell'Ufficio Formazione. Solo successivamente andrà in copia al Manager HSE, al Datore di Lavoro o al suo Delegato e all'AD di riferimento.

- **UFFICIO SICUREZZA E RISK MANAGEMENT**
  - le richieste da € 0 a € 25.000,00 sono inserite e approvate direttamente dal Risk Manager e in c.c. all'AD.
  - le richieste oltre € 25.001,00 devono essere approvate anche dall'AD.

Per gli acquisti relativi al campo di applicazione del D.lgs. 269/2010 nonché a quelli relativi alla sicurezza fisica e tecnologica è necessario ottenere il parere obbligatorio e vincolante del Risk&Regional Security Manager per la valutazione della conformità dei prodotti, con l'approvazione finale dei soggetti preposti all'acquisto, salvo che le richieste oppure le RDA provengano direttamente dall'Ufficio Sicurezza con in copia il Risk&Regional Security Manager anche via mail, nel qual caso il parere si intende automaticamente acquisito e verificato.

Per quanto attiene agli acquisti strettamente correlati all'operatività societaria, si riportano di seguito i workflow autorizzativi per gli acquisti afferenti alla Vigilanza e all'Assistenza Tecnica commerciale:

- **VIGILANZA**
  - per acquisti di importo inferiore a 1.500,00 €, il Responsabile di Filiale/Sede/ Coordinatore non necessita di autorizzazioni e gestisce le Richieste di Approvvigionamento in maniera autonoma e comunque mediante l'utilizzo del sistema informatico che prevede l'invio in copia conoscenza al Responsabile Operativo o superiore;
  - per acquisti di importo compreso tra i 1.501,00 e i 10.000,00 €, il Responsabile Operativo valuta l'effettiva necessità, sottoscrive elettronicamente per conferma e accettazione l'Ordine di Acquisto, inoltrando automaticamente la comunicazione per conoscenza al Direttore di Divisione (o AD di riferimento);
  - per acquisti di importo compreso tra i 10.001,00 € e i 25.000 €, il Direttore di Divisione o di Funzione (o l'AD di riferimento) accerta l'effettiva necessità, sottoscrive elettronicamente per conferma e accettazione l'Ordine di Acquisto, inoltrando automaticamente la comunicazione per conoscenza all'Amministratore di riferimento se non coincidente con lo stesso;
  - per acquisti di importo superiore ai 25.000,00 €, l'Amministratore Delegato di riferimento, dopo le opportune verifiche, e constatata l'effettiva necessità, provvede a sottoscrivere elettronicamente per conferma e accettazione l'Ordine di Acquisto.

È facoltà dei Direttori di Divisione o Amministratori Delegati di riferimento disporre, con propria disposizione scritta, che le spese vengano dagli stessi autorizzate e sottoscritte anche per acquisti di importo inferiore a quanto sopra stabilito, in aggiunta alle autorizzazioni previste dalla presente procedura. La sola autorizzazione del Direttore di Divisione non completa il processo di acquisto.

- **ASSISTENZA TECNICA COMMERCIALE**

Tipologie di acquisti:

1. INSTALLAZIONE IMPIANTI:
   A) Con materiale fornito da Rangers
   B) Con materiale fornito dall'installatore (anche a canone)

2. ASSISTENZA E MANUTENZIONE (solo attività di manodopera con eventuale sostituzione di consumabile)

3. ACQUISTO MATERIALE (fattura mensile tranne per Amazon)

4. ALTRI COSTI (canoni di locazione: esempio ponti radio e connettività)

- In sostituzione dell'RDA viene generato dall'Assistenza Tecnica Commerciale un report PDF automaticamente dal portale FRS che riepiloga le installazioni effettuate nel mese di competenza che rispecchia il totale fatturato dal singolo fornitore. Il documento dovrà essere sottoscritto con le fasce autorizzative riepilogate in calce.
- Come nel caso precedente.
- In sostituzione dell'RDA viene generato dall'Assistenza Tecnica Commerciale un report PDF automaticamente dal modulo acquisti in Freeway che riepiloga gli ordini effettuati e consegnati nel mese di competenza che rispecchia il totale fatturato dal singolo fornitore. Il documento dovrà essere sottoscritto con le fasce autorizzative riepilogate in calce.
- Viene superata la necessità delle RDA. Questa attività è ritenuta del tutto superflua, in quanto – una volta autorizzato il contratto principale secondo i parametri autorizzativi previsti, la conferma delle tariffe mensile non necessita di singole specifiche RDA ma solamente di una conferma del canone che può essere effettuata direttamente dall'amministrazione (come ad esempio nel caso dei corrispondenti e dei contratti di locazione immobiliare).

Fasce autorizzative

ASSISTENZA E MANUTENZIONE / INSTALLAZIONI E ACQUISTO MATERIALI (1, 2, 3)

- Da 0 a 5.000,00 euro Responsabile Assistenza Tecnica Commerciale;
  Oltre i 5.000,00 euro Responsabile Assistenza Tecnica Commerciale e A.D..

L'Ufficio competente emette l'Ordine di Acquisto al fornitore scelto a valle della valutazione delle offerte pervenute e dell'autorizzazione di spesa ottenuta. Gli Ordini di Acquisto sono identificati in maniera univoca da un codice numerico assegnato in automatico dal sistema informativo.

Il procedimento di comparazione non è obbligatorio in alcuni casi specifici, per i quali si rinvia alla Policy approvvigionamenti.

Le eventuali attività sospette sono segnalate all'Organismo di Vigilanza e al Consiglio di Amministrazione.

7.3 GESTIONE DEI RAPPORTI CONSULENZIALI

I rapporti consulenziali sono gestiti nel rispetto della vigente normativa, in applicazione dei generali principi di trasparenza e correttezza e in applicazione delle procedure previste dal Manuale della Qualità che vengono qui integralmente richiamate.

L'assegnazione di incarichi professionali a consulenti deve rispondere a reali esigenze aziendali e la corresponsione di compensi o provvigioni deve essere congrua rispetto alle prestazioni rese alla Società e in linea con l'incarico conferito.

La scelta dei consulenti avviene mediante procedimento di referenziamento che tenga conto di:

- ambito di specializzazione del singolo professionista;
- documentata e comprovata competenza professionale;
- organizzazione della quale il professionista si avvale;
- adeguatezza dei compensi richiesti.

I consulenti sono tenuti al rigoroso rispetto della normativa vigente e dei princìpi espressi nel Codice Etico.

I contratti con tali soggetti devono contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e in particolare delle norme comportamentali sancite nel Codice Etico della Società e di impegno al loro rispetto. A tale proposito i contratti dovranno essere integrati con la seguente clausola generale, adattata in base allo specifico rapporto contrattuale: "*Il professionista dichiara di conoscere le prescrizioni contenute nel Codice Etico adottato dalla Società e dichiara, inoltre, di accettarle integralmente, astenendosi da comportamenti a esse contrari. Il professionista, nel caso in cui sia dipendente o collabori con enti pubblici, dichiara di aver assolto tutti gli adempimenti da questi eventualmente richiesti e/o previsti dalle leggi in vigore per l'assunzione di altri incarichi professionali. L'eventuale inosservanza di tali principi potrà costituire inadempimento contrattuale, legittimando la Società a risolvere il presente contratto ai sensi e per gli effetti dell'articolo 1456 del Codice Civile, fermo restando il diritto al risarcimento dei danni eventualmente subiti dalla Società per effetto di detto inadempimento.*"

La violazione del Codice Etico da parte del consulente comporta la risoluzione del contratto con effetto dal momento dell'accertamento, residuando in capo alla Società il diritto al risarcimento del danno.

L'assegnazione di incarichi consulenziali è subordinata ad autorizzazione di spesa da parte dei soggetti titolari del potere di disporre spese, secondo le soglie autorizzative previste dalle procedure

aziendali, e previa verifica dei necessari requisiti di professionalità, qualità della prestazione e congruità del corrispettivo richiesto.

Tra la Società e il consulente deve sussistere apposito contratto, conservato in apposito fascicolo (cartaceo o informatico). In quest'ultimo è altresì mantenuta la documentazione concernente lo sviluppo dell'incarico consulenziale, le parcelle emesse dal consulente e le relative disposizioni di pagamento.

La Società prevede:

- verifiche sul compenso corrisposto rispetto a quanto accordato;
- monitoraggio delle attività svolte.

Ogni anomalia deve essere tempestivamente comunicata all'Organismo di Vigilanza. L'Organismo di Vigilanza ha facoltà di verificare la corretta applicazione di tale procedura.

7.4GESTIONE DEI CORRISPONDENTI

La Società, nell'ambito dei servizi di vigilanza e trasporto, affida a società esterne operanti nei medesimi settori (cd. corrispondenti) parte dei servizi da erogare ai clienti.

Le unità organizzative preposte effettuano periodicamente ricerche di mercato al fine di individuare potenziali corrispondenti da contrattualizzare, muniti dei necessari requisiti tecnici/organizzativi in grado di soddisfare i fabbisogni della Società.

Il processo di valutazione comporta un'analisi interna e, laddove ritenuto necessario, può prevedere visite presso il potenziale fornitore; la valutazione si fonda sui dati e le informazioni di carattere generale, tecnico, economico, finanziario, nonché di conformità alla legislazione vigente, utili ad accertare quali siano i requisiti posseduti.

I principali parametri oggetto di valutazione sono:

- capacità di erogazione dei servizi, in termini di disponibilità di uomini e mezzi;
- conformità ai requisiti della legislazione vigente;
- adeguatezza strutture di sicurezza;
- capacità assicurativa idonea;
- adozione di adeguati strumenti di *compliance*;
- ambito territoriale di riferimento.

Ai fini della selezione del corrispondente, il Direttore Commerciale si occupa della raccolta delle offerte, della valutazione preventiva e della comparazione tra potenziali fornitori, attenendosi ai principi di comportamento sopra riportati; una volta individuato il soggetto idoneo, il relativo contratto viene sottoposto all'attenzione del Presidente del CdA o di un Amministratore delegato perla firma.

Nei casi in cui non sia possibile operare una comparazione tra più offerte, per esempio per unicità del corrispondente in relazione a uno specifico ambito geografico o per specificità delle dotazioni tecniche richieste, ne viene data adeguata evidenza scritta, riferendo al Presidente del CdA o a un Amministratore Delegato.

Preventivamente alla stipula dell'accordo, ai fornitori selezionati sono richiesti i documenti attestanti la conformità alla normativa vigente. Il tariffario concordato è sottoscritto da parte del personale dotato di idonei poteri. I tariffari sottoscritti e l'elenco aggiornato dei corrispondenti contrattualizzati sono redatti e monitorati da parte dell'Ufficio Corrispondenti.

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Al fine di verificare il rispetto delle procedure relative al processo in oggetto, i Responsabili delle Funzioni interessate inviano all'Organismo di Vigilanza, con periodicità definita dallo stesso, apposite relazioni, segnalando eventuali ipotesi di anomalie verificatesi ma non oggetto di immediata segnalazione.

Inoltre, chiunque rilevi anomalie nello svolgimento delle attività oggetto del presente Protocollo è tenuto a informare tempestivamente l'Organismo di Vigilanza sulle criticità riscontrate.

Conformemente a quanto stabilito nella Parte Generale del Modello 231, fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli di propria iniziativa o a seguito delle segnalazioni ricevute, esso effettua periodicamente controlli a campione sulle attività di "Gestione degli approvvigionamenti", diretti a verificare il rispetto delle procedure indicate.

9. CONSERVAZIONE DELLA DOCUMENTAZIONE

I Responsabili delle Funzioni coinvolte nelle attività sensibili individuate nel presente Protocollo sono responsabili, ciascuno per la parte di propria competenza, della conservazione della documentazione, nel rispetto dei termini di legge, al fine di garantire la tracciabilità delle operazioni aziendali. La documentazione è, inoltre, messa a disposizione, su richiesta, del Presidente del CdA, dell'Amministratore Delegato, del Consiglio di Amministrazione e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

SELEZIONE, ASSUNZIONE E GESTIONE DEL PERSONALE

INDICE

1. FINALITÀ 2

2. IL SISTEMA DEI CONTROLLI 2

2.1. STANDARD DI CONTROLLO GENERALI 2
2.2 STANDARD DI CONTROLLO SPECIFICI 3

3. AMBITO DI APPLICAZIONE 4

4. NORMATIVA DI RIFERIMENTO 4

5. REATI ASTRATTAMENTE PERPETRABILI 5

6. REGOLE GENERALI DI COMPORTAMENTO 11

7. PRESIDI DI CONTROLLO 13

7.1 SELEZIONE E ASSUNZIONE DEL PERSONALE DIPENDENTE 13
7.2 SELEZIONE E ASSUNZIONE DI GUARDIE PARTICOLARI GIURATE 16
7.3 SICUREZZA DEI LAVORATORI 17
7.4 GESTIONE DELLE NOTE DI SPESA E DELLE SPESE DI RAPPRESENTANZA 17
7.5 GESTIONE DELLA SEGNALAZIONE DI SINISTRI 18
7.6 MODIFICA DEGLI ORGANIGRAMMI 18

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA 19

9. CONSERVAZIONE DELLA DOCUMENTAZIONE 19

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il Personale deve attenersi nell'ambito del processo di "**Selezione, Assunzione e Gestione del Personale**".

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice Etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società, nelle procedure e istruzioni operative e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi Sociali, i Dipendenti, i Collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;
- Fornire all'OdV e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei Dipendenti –in via diretta – dei Collaboratori Esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione-di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da - considerati individualmente o collettivamente - integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee guida di Confindustria, nonché delle "*bestpractice*", prevede con riferimento alle Aree e alle Attività Sensibili individuate:

- *standard di controllo "generali"*, applicabili a tutte le Attività Sensibili;
- *standard di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

2.1. STANDARD DI CONTROLLO GENERALI

- Gli *standard* di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:
- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;

- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa- Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

2.2 STANDARD DI CONTROLLO SPECIFICI

Sulla base degli *standard* di controllo generali sopra riportati, gli *standard* di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;
- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema delle deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità

delle sottostanti operazioni economiche.

3. AMBITO DI APPLICAZIONE

Il presente Protocollo si applica a Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 ed è rivolto a tutti i soggetti aziendali coinvolti, a vario titolo, nel processo di "Selezione, Assunzione e Gestione del Personale e delle Guardie Particolari Giurate". Concerne, in particolare, tutte quelle funzioni/uffici interessati e coinvolti nei seguenti processi:

- Selezione del Personale;
- Assunzione del Personale;
- Selezione e assunzione delle Guardie Particolari Giurate (G.P.G.);
- Sicurezza dei lavoratori;
- Attribuzione degli emolumenti e rimborso spese;
- Gestione dei sinistri stradali.

Il Responsabile della Direzione Risorse Umane Corporate è il soggetto che ha la responsabilità della diffusione del presente Protocollo di conformità ai propri collaboratori e il compito di garantirne la continua applicazione e il costante aggiornamento.

Le Funzioni aziendali coinvolte a qualsiasi titolo nella presente procedura sono:

- Direzione Risorse Umane Corporate
- Ufficio del personale;
- Consiglio di Amministrazione;
- Titolare di licenza;
- Responsabili di Funzione/Direzione;
- Responsabile servizio prevenzione e protezione (RSPP);
- Responsabile sistemi di sicurezza e innovazione
- Datore di Lavoro e suo delegato;
- Responsabile del sistema di gestione della salute e della sicurezza sul lavoro (RSGSL);
- Responsabile di conformità per la prevenzione della corruzione (RAC);
- Responsabile dell'Organizzazione Aziendale.

4. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30"*;
- D.lgs. 9 aprile 2008 n. 81 *"Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro"*;
- Legge 12 marzo 1999, n. 68 "*Norme per il diritto al lavoro dei disabili*";

- Regio Decreto 18 giugno 1931, n. 773, "*Testo unico delle Leggi di Pubblica Sicurezza*";
- R.D.L. 26/9/1935 n. 1952 convertito in Legge 508/36 "*Disciplina del servizio delle Guardie Particolari Giurate*".

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;
- Protocollo "Gestione degli adempimenti previsti in materia di sicurezza e salute sul lavoro";
- Codice Etico del Gruppo Battistolli;
- Procedure e istruzioni operative;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Policy "Gestione dei sinistri stradali";
- Sistema di gestione di prevenzione della corruzione (UNI ISO 37001:2016);
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

5. REATI ASTRATTAMENTE PERPETRABILI

I reati presupposto (nella forma consumata o tentata) di cui al D.lgs. 231/01 da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati:

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25):**
  - Malversazione di erogazioni pubbliche (art. 316-*bis* c.p.);

Il reato di malversazione a danno dello Stato si perfeziona quando s'impiegano contributi, sovvenzioni, mutui agevolati o finanziamenti pubblici (statali, di altri enti pubblici o comunitari) ottenuti per la realizzazione di opere e attività di vario interesse, per finalità diverse da quelle per le quali sono stati erogati. L'ipotesi criminosa si caratterizza per l'ottenimento di finanziamenti pubblici in modo lecito e per il successivo utilizzo degli stessi per finalità diverse da quelle sottese all'erogazione. Il delitto può essere commesso da chiunque, estraneo alla P.A. ometta di destinare, anche parzialmente, i fondi già ottenuti alle finalità per le quali gli stessi sono stati erogati. L'elemento soggettivo richiesto per l'integrazione della fattispecie è il dolo generico, sicché è sufficiente la consapevolezza della provenienza dei fondi e la volontà di non impiegare gli stessi per le finalità per le quali erano stati concessi.

  - Indebita percezione di erogazioni pubbliche (art. 316-*ter* c.p.);

Il reato in esame si concretizza nell'indebito conseguimento, per sé o per altri, di fondi, comunque denominati, concessi o erogati dallo Stato, da altri Enti pubblici o dalle Comunità europee, mediante l'utilizzo o nella presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero nella omissione di informazioni dovute. A differenza della malversazione, dunque, la fattispecie in esame riguarda il conseguimento indebito dei finanziamenti, senza che a nulla rilevi l'uso che poi venga fatto delle erogazioni. In breve, mentre la malversazione integra le ipotesi d'indebito utilizzo di fondi regolarmente erogati e conseguiti, l'art. 316 ter punisce le attività connesse a un momento precedente, ossia quello di un'indebita percezione dei fondi.

  - Concussione (art. 317 c.p.);

Il reato di concussione si caratterizza per l'utilizzo indebito da parte del funzionario pubblico dei propri poteri, al fine di costringere il soggetto passivo a riconoscere al funzionario o ad un terzo soggetto un vantaggio di natura economica o personale. Si ha abuso dei poteri quando gli stessi siano esercitati fuori dei casi previsti da leggi, regolamenti e istruzioni di servizio o senza le forme prescritte, ovvero quando detti poteri, pur rientrando tra quelli attribuiti al pubblico ufficiale, vengano utilizzati per il raggiungimento di scopi illeciti.

- Truffa in danno dello Stato o di un ente pubblico (art. 640, comma 2, n. 1, c.p.);

L'ipotesi si configura nel caso in cui un qualunque soggetto, con artifici o raggiri tali da indurre in errore la controparte, procura a sé o ad altri un ingiusto profitto con danno dello Stato o di altro Ente pubblico. Trattasi di reato a dolo generico, sicché per la consumazione dello stesso è necessario che ricorrano tanto il profitto per il privato quanto il danno per lo Stato; l'assenza di tali elementi determina la necessaria qualificazione delle condotte fraudolente come ipotesi di truffa tentata e non consumata.

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

La fattispecie in oggetto consta dei medesimi elementi costitutivi della truffa semplice (art. 640 c.p.) ma rappresenta più grave ed autonoma fattispecie in quanto l'ingiusto profitto per il privato è rappresentato da contributi, sovvenzioni, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri Enti pubblici o delle Comunità europee. Tale ipotesi si distingue dunque da quella prevista e punita ex art. 640, co. 2 n. 1 c.p. per la diversa natura del profitto, mentre si distingue dall'ipotesi di cui all'art. 316 ter c.p. per le diverse e più gravi modalità della condotta, che nella fattispecie in esame risulta più marcatamente connotata da comportamenti fraudolenti. Con la sentenza n. 5150/2013, la Corte di Cassazione ha affermato che in caso di procedimento "231" a seguito di truffa ai danni dello Stato per il conseguimento di pubbliche erogazioni, è legittimo il sequestro operato in capo al soggetto che, pur non essendo il diretto richiedente dell'erogazione, ne risulta il destinatario finale, in virtù di un rapporto a carattere privato con il ricevente principale. Segnatamente, il finanziamento pubblico era stato ricevuto da un soggetto privato che, mediante la sottoscrizione di contratti di appalto, lo ha a sua volta corrisposto alla società in questione. Tuttavia, secondo la Suprema Corte, la presenza di un "intermediario" non sarebbe sufficiente a far venir meno il carattere pubblico della somma di denaro.

- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.);

L'intervento manipolativo può essere tale da modificare gli scopi cui il sistema informatico è destinato, ma il reato ricorre anche quando - pur nel rispetto della destinazione del sistema - sono manipolati i contenuti dello stesso. Diversamente, la condotta alternativa di 'intervento abusivo' è rivolta ai dati, alle informazioni (cioè, per semplificare, ad un insieme di dati) o ai programmi (software) installati nell'hardware. In particolare, va rilevato che l'intervento, per configurare la condotta descritta dalla fattispecie ex art. 640 ter c.p., deve avvenire "senza diritto" e, dunque, non solo in assenza del necessario consenso del titolare dei dati, informazioni e programmi contenuti nel sistema informatico, ma anche secondo una modalità non consentita da norme giuridiche, né da altre fonti. Il reato di frode informatica presenta, in breve, la medesima struttura e i medesimi elementi costitutivi del reato di truffa da cui si distingue in quanto l'attività illecita investe non la persona ma un sistema informatico. Nel reato di frode informatica, pertanto, non assume rilevanza - a differenza che nel reato di truffa - il ricorso da parte dell'autore del reato ad artifizi o raggiri, ma l'elemento oggettivo dell'alterazione del sistema informatico (e/o dei dati in esso disponibili).

- Corruzione (artt. 318, 319, 320, 322-*bis* c.p.);

Il reato di corruzione consiste in un accordo fra un pubblico funzionario e un privato, in forza del quale il primo accetta dal secondo un compenso che non gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria). Nella corruzione il pubblico ufficiale ed il privato sono in posizione paritaria, diversamente dalla concussione che invece presuppone lo sfruttamento da parte del funzionario della propria posizione di superiorità alla quale corrisponde una situazione di soggezione nel privato. La fattispecie prevista dall'art. 319 c.p., connotata come quella di cui all'art. 318 c.p. da un rapporto paritetico tra pubblico ufficiale/ incaricato di un pubblico servizio-corrotto e privato-corruttore, se ne differenzia in virtù del fatto che l'atto richiesto al pubblico ufficiale o all'incaricato di un pubblico servizio a fronte della dazione o della promessa di denaro o di altra utilità, risulta contrario ai doveri d'ufficio. In particolare la condotta può concretizzarsi in una omissione o in un ritardo nel compimento di un atto di ufficio ovvero nel compimento di un atto contrario ai doveri di ufficio.

- Istigazione alla corruzione (art. 322 c.p.);

Il reato è configurabile solo ove l'offerta del privato o la richiesta del pubblico funzionario non vengano accolte dal destinatario. Tuttavia, ove il rifiuto non sia stato immediato e siano incorse trattative poi non sfociate in un accordo, si ritiene configurabile un tentativo di corruzione del quale rispondono entrambi i soggetti. Nell'istigazione alla corruzione passiva la condotta consiste nell'offrire o nel promettere denaro o altra utilità non dovuti al funzionario. L'offerta o la promessa deve essere seria e concreta ed idonea alla realizzazione dello scopo, tale cioè da indurre il destinatario a compiere o a ritardare un atto dell'ufficio o del servizio ovvero a fare un atto contrario a detti doveri. L'idoneità dell'offerta va valutata con un giudizio "ex ante" che tenga conto dell'entità del compenso, delle qualità personali del destinatario e della sua posizione economica e di ogni altra connotazione del caso concreto.

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

Per quanto riguarda il reato di corruzione in atti giudiziari (art. 319 ter c.p.), si precisa che tale fattispecie non ricorre soltanto in relazione all'esercizio delle funzioni giudiziarie cui è subordinata e allo status di colui che le esercita, ma ha una portata più ampia. Infatti, come precisato dalla Corte di Cassazione, costituisce "atto giudiziario" qualsiasi atto funzionale a un procedimento giudiziario, indipendentemente dalla qualifica soggettiva di chi lo realizza (cfr. Cass., Sezioni Unite, sentenza n. 15.208 del 25/2/2010, con riferimento alla testimonianza resa in un processo penale).

- Corruzione tra privati (art. 2635 c.c.).

La nuova formulazione dell'art. 2635 c.c. estende il novero dei soggetti attivi includendo tra gli autori del reato, oltre a coloro che rivestono posizioni apicali di amministrazione o di controllo, anche coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive presso società o enti privati. Ai fini "231", per quanto concerne la corruzione tra privati, resta reato-presupposto la sola fattispecie di cui al comma 3 dell'articolo 2635 del codice civile, cioè il delitto commesso da chi corrompe, oggi anche per interposta persona, i soggetti indicati nel primo comma del medesimo articolo (nella sua nuova e più estesa versione) per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

- Frode nelle pubbliche forniture (art. 356 c.p.);

Tale fattispecie punisce chiunque commette frode nell'esecuzione dei contratti di fornitura conclusi con lo Sato, con un Ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità. Per giurisprudenza e dottrina costante è richiesto un inadempimento dell'obbligazione parziale o inesatto ma anche in un adempimento totale. La condotta consiste nella frode nel corso dell'esecuzione di uno dei contratti indicati nell'art. 255 e pertanto devono riguardare cose od opere necessarie a unostabilimento pubblico o a un pubblico servizio.

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

Il reato si configura quando un pubblico ufficiale o un incaricato di un pubblico servizio si appropria di denaro o di altra cosa mobile altrui, di cui lo stesso è in possesso per ragione del suo ufficio o servizio. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

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

Il reato punisce il pubblico ufficiale o l'incaricato di un pubblico servizio, che, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

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

Tale reato punisce, salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea. Il reato è imputabile all'ente solo quando il fatto offende gli interessi finanziari dell'Unione Europea.

La fattispecie potrebbe realizzarsi, in concreto, nel caso in cui un dipendente dell'impresa, approfittando di rapporti personali con il funzionario pubblico preposto al rilascio di determinati permessi e/o autorizzazioni, prenda contatto con quest'ultimo per ottenere un provvedimento favorevole nell'interesse dell'impresa, pur consapevole di non averne diritto. Il dipendente (e con lui l'impresa nel cui interesse lo stesso abbia agito) risponderebbe a titolo di concorso dell'extraneus nel reato "proprio".

- **Reati in materia di ricettazione, riciclaggio e impiego di denaro di provenienza illecita, introdotti dal D.lgs. 231/2007 (art. 25-*octies*):**
  - Ricettazione (art. 648 c.p.)

L'incipit della norma, in relazione al soggetto attivo, esclude che possa essere autore della ricettazione colui che ha commesso il reato da cui i beni provengono. Dunque chi commissiona il delitto presupposto concorre nella sua realizzazione come istigatore ed è punibile a tale titolo, mentre la successiva condotta di ricezione rileva come mero post factum non punibile. L'oggetto materiale è costituito da denaro o cose provenienti da delitto. La giurisprudenza vi comprende i servizi, l'energia o programmi di *know how*, mentre si divide riguardo gli immobili. Infine, riguardo ai rapporti con le figure concorrenti, si può tendenzialmente affermare che la ricettazione è destinata a lasciare spazio alle previsioni che incriminano specificamente la ricezione di un determinato bene di origine illecita. Ad esempio, in applicazione del principio di specialità *ex* art. 15 c.p., gli artt. 453, n. 3/4 e 455 c.p., che sanzionano chi acquista, riceve o detiene monete contraffate o alterate al fine di metterle in circolazione, sono destinati a prevalere sull'art. 648 c.p.

  - Riciclaggio (art. 648-*bis* c.p.)

Anche ai fini della configurabilità del reato di riciclaggio è necessario che sia in precedenza consumata altra fattispecie criminale. Più precisamente, affinché vi sia un provento illecito da riciclare – sia esso denaro o altro bene o utilità – è imprescindibile il fatto che un reato, per l'appunto presupposto sia stato commesso. Il riciclaggio consiste, quindi, nelle attività volte a dissimulare l'origine illecita dei proventi criminali ed a creare l'apparenza che la loro origine sia lecita.

- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.)

Chi impiega denaro di provenienza delittuosa, direttamente in un'attività economica o finanziaria, così ripulendolo, risponde non del reato di riciclaggio, ma di quello punito dall'art. 648-ter c.p. appunto «Impiego di denaro, beni o utilità di provenienza illecita». In quest'ultimo, infatti, è "assorbita" la precedente attività di sostituzione o di ricezione. Invece, se taluno sostituisce denaro di provenienza illecita con altro denaro o altre unità e, poi, impieghi i proventi derivanti da tale opera di ripulitura in attività economiche o finanziarie, risponde del solo reato di riciclaggio (art. 648 bis c.p.) con esclusione del 648-ter c.p.

- Autoriciclaggio (art. 648-*ter* 1 c.p.)

Il delitto di riciclaggio, così come formulato dall'art. 648- bis c.p., punisce chi ricicla denaro, beni o altre utilità provenienti da un delitto non colposo commesso da un altro soggetto, mentre nessuna sanzione era prevista per chi ricicla in prima persona , cioè sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo da egli commesso (o che ha concorso a commettere), ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. L'introduzione del reato di autoriciclaggio è stata necessaria per colmare questa lacuna nel nostro ordinamento. Il delitto di autoriciclaggio, peraltro, prevede pene diverse a seconda della gravità del delitto presupposto e con previsione della non punibilità delle condotte nelle quali il denaro, i beni o le altre utilità vengono destinati «alla mera utilizzazione o al godimento personale».

- **Delitti in materia di strumenti di pagamento diversi dai contanti, introdotti dal D.Lgs. 184/2021 (art. 25 octies I):**

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter, co. I c.p.).

Il delitto di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, così come formulato dall'art. 493 ter, co. I c.p., punisce chi indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti. La norma contempla, altresì, l'ipotesi del soggetto che falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. La novella del legislatore estende il campo della condotta, contemplando ogni strumento di pagamento diverso dal contante che sia idoneo ad abilitare al prelievo del denaro o all'acquisto di beni o prestazione di servizi o comunque rappresenti uno strumento di pagamento diverso dal contante.

- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater, co. I c.p.).

La norma contempla l'ipotesi in cui, salvo che il fatto costituisca più grave reato, il soggetto che, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti,produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

- **Reati contro la personalità individuale, introdotti dalla legge 228/2003, e modificati con la legge 38/2006, e dalla legge 199/2016 (art. 25-*quinquies*):**

  - Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)

La norma descrive due ipotesi delittuose. La prima riconduce alla nozione di "schiavitù" "l'esercizio su una persona di poteri corrispondenti a quelli del diritto di proprietà". Quindi sono compresi sia le tipiche facoltà inerente al diritto di proprietà, cioè godere e disporre, sia l'esercizio di diritti reali minori. Invece la seconda figura prescinde dal richiamo al diritto domenicale e si distingue due momenti: lo sfruttamento coattivo di una persona e la condizione di assoggettamento dall'altro. La sinergia tra queste due condizioni permette di individuare il reato de quo quando la persona diventa una "cosa" poiché la sua vita è interamente determinata a sistematicamente finalizzata per la realizzazione di utilità godute da soggetti terzi. *Ex* D.lgs. 231/2001, la condotta rilevante in questi casi è costituita dal procacciamento illegale della forza lavoro attraverso il traffico di migranti e la tratta degli schiavi.

  - Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.)

Il reato in esame, oggi, risulta slegato dal requisito dello svolgimento di «*un'attività organizzata di intermediazione*», andando a colpire non solo chi «*recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento...*», ma altresì chiunque «*utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno*». Anche gli "indici di sfruttamento" enunciati dall'art. 603-bis c.p. assumono una connotazione più ampia, essendo oggi alcuni di essi parametrati, ad esempio, non più a condotte sistematiche di sotto retribuzione e violazione delle norme su orari, riposi, aspettativa e ferie, bensì a siffatte condotte anche solo «reiterate». La punibilità dell'ente è dunque collegata al compimento di un reato non più limitato a chi svolge attività organizzata d'intermediazione, né legato a violenza e minaccia come elementi costitutivi. Reato connotato inoltre da «uno sfruttamento» la cui presenza è dedotta dalla semplice reiterazione di condotte di retribuzione palesemente difforme dai contratti collettivi nazionali o territoriali, dalla violazione delle norme su orario, riposo, aspettativa e ferie o dalla mera sussistenza di violazione delle norme antinfortunistiche, anche non tali da esporre a pericolo il lavoratore. A contemperamento di una siffatta estensione nella possibile applicazione della norma, si deve tuttavia considerare la natura dolosa del reato in esame, con la conseguenza che le condotte costituenti "indice di sfruttamento" rileveranno solo ove dolosamente preordinate a sottoporre «i lavoratori a condizioni di sfruttamento» con consapevolezza e volontà di approfittare «del loro stato di bisogno».

- **Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies*)**

Esempio: vengono disposte assunzioni di personale straniero irregolare al fine di ottenere una gestione "facilitata" dello stesso personale soggiogato dalla condizione di irregolarità.

Al fine di contrastare la realizzazione della fattispecie di reato, è stata predisposta apposita regolamentazione "7.1.1 ASSUNZIONE DEL PERSONALE DIPENDENTE STRANIERO" per la cui procedura è richiesta una verifica e predisposizione della documentazione relativa alla posizione dello straniero sia nel momento antecedente l'assunzione che in itinere durante il rapporto lavorativo.

Ai sensi dell'art. 25-duodecies, comma 1-bis, la condotta tipica è quella di colui il quale ("chiunque") promuova, diriga, organizzi, finanzi o effettui il trasporto di stranieri nel territorio dello Stato ovvero compia altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di un altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente e nel caso in cui: il fatto riguardi l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone; la persona trasportata sia stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale; la persona trasportata sia stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale; il fatto sia commesso da tre o più persone in concorso fra loro utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti; gli autori del fatto abbiano la disponibilità di armi o materie esplodenti. L'art. 25-duodecies, comma 1-ter, prevede invece il caso in cui un soggetto, agendo nell'interesse o a vantaggio della società, al fine di trarre un ingiusto profitto dalla condizione d'illegalità dello straniero o nell'ambito delle attività punite a norma dell'art. 12 D.Lgs. 286/1998, favorisca la permanenza dello straniero nel territorio dello Stato in violazione delle norme del Testo Unico sull'immigrazione.

- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25-decies)**

Il bene giuridico tutelato è rappresentato dall'interesse alla genuinità della prova, così come dal corretto svolgimento dell'amministrazione della giustizia. Più in particolare, il legislatore ha voluto reprimere tutte quelle condotte in grado di creare influenze esterne per turbare la ricerca della verità nel processo. L'elemento psicologico del reato è rappresentato dal dolo specifico, inteso come la coscienza e la volontà del fatto tipico, con l'ulteriore scopo di indurre taluno a comportarsi in un determinato modo. La fattispecie incriminatrice ha anche una natura sussidiaria in quanto trova applicazione soltanto quando il fatto non è riconducibile ad un'altra figura criminosa. Inoltre, l'elemento oggettivo del reato è rappresentato da una condotta che consiste nell'uso della violenza o minaccia oppure nella promessa del denaro o altra utilità al fine delineato e descritto dalla disposizione in oggetto.

Esempio: al dipendente sono impartite istruzioni illecite, mediante pressioni, promesse o minacce, circa le dichiarazioni da rendere o da tacere in caso di coinvolgimento dinanzi all'Autorità Giudiziaria.

Al fine di contrastare la realizzazione della fattispecie è predisposto apposito iter "7.1.2 INFORMAZIONE E FORMAZIONE DEL NEO ASSUNTO" di cui risultano investiti gli organi societari al fine di rendere edotto il dipendente degli obblighi di legge connessi al d.lgs. 231/01, Codice etico, PTCP ed altra documentazione inerente l'opera di sensibilizzazione informativa e formativa.

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

6. REGOLE GENERALI DI COMPORTAMENTO

Coerentemente con i princìpi deontologici previsti dalCodice Etico, il Personale deve fare riferimento alle norme comportamentali di seguito individuate.

- La selezione del Personale è effettuata in base alle esigenze aziendali e alla corrispondenza con i profili professionali ricercati, riconoscendo pari opportunità per i candidati.

- Le informazioni richieste in sede di selezione sono strettamente collegate alla verifica del profilo professionale e psicoattitudinale ricercato, nel rispetto della sfera privata del candidato e delle sue opinioni personali. Non può costituire oggetto del colloquio l'analisi delle condizioni economiche personali del lavoratore o la valutazione del suo stato di bisogno.
- La Società si avvale esclusivamente di Personale assunto in conformità alle tipologie contrattuali previste dalla normativa e dai contratti collettivi nazionali o territoriali di lavoro applicabili stipulati dalle associazioni sindacali più rappresentative a livello nazionale.
- La Società, laddove necessario, si avvale esclusivamente di intermediari autorizzati per la selezione del Personale.

L'accesso ai ruoli e agli incarichi è definito in considerazione dell'affidabilità (in termini di diligenza e fedeltà), delle competenze e delle capacità dei singoli, sulla base delle specifiche esigenze della Società e senza discriminazione alcuna, compatibilmente con i criteri di efficienza generale del lavoro.

Salvo espressa e motivata deroga del CdA, previo parere non vincolante dell'Organismo di Vigilanza, non possono essere assunti presso la Società:

- pubblici dipendenti con i quali negli ultimi due anni la Società abbia intrattenuto rapporti commerciali o comunque inerenti all'attività degli stessi pubblici dipendenti, loro parenti o affini o persone a esse legate anche da un rapporto di amicizia o di interesse;
- soggetti che ricoprono cariche pubbliche o che svolgono incarichi pubblici tali da poterli porre in una situazione di conflitto di interessi, loro parenti o affini o persone a esse legate anche da un rapporto di amicizia o di interesse;
- soggetti che hanno rapporti di parentela con dipendenti della Società;
- soggetti che hanno rapporti di parentela con individui che hanno svolto attività di verifica o ispezione nei precedenti 24 mesi.

È, in ogni caso, fatto tassativo divieto a chiunque di promettere o concedere promesse d'assunzione, in favore di:

- rappresentanti della Pubblica Amministrazione;
- loro parenti o affini;
- persone segnalate dai soggetti di cui ai punti precedenti;

al fine di influenzare l'indipendenza di giudizio dei rappresentanti della Pubblica Amministrazione o di indurli ad assicurare un qualsiasi vantaggio per la Società.

I *benefit* sono gestiti nel rispetto della normativa previdenziale, contributiva e fiscale in materia.

Qualora la Società si avvalga di società esterne per l'espletamento di attività legate alla gestione del Personale, i contratti con tali società devono contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e di impegno al suo rispetto e all'osservanza dei principi contenuti nel Codice Etico adottato da Rangers S.r.l..

Alla luce delle recenti modifiche legislative al decreto 231/01, mediante la legge 199/2016, che ha introdotto tra i reati presupposto la fattispecie del "caporalato", è fatta espressa richiesta ai soggetti aziendali (Datore di Lavoro) e agli Uffici aziendali a vario titolo coinvolti nella attività di selezione, assunzione e gestione del Personale, di:

- avvalersi esclusivamente di intermediatori autorizzati per la selezione del Personale;
- erogare a tutto il Personale assunto, utilizzato o impiegato, una retribuzione non difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale e comunque non difforme dalla qualità e quantità del lavoro prestato;
- effettuare la gestione di tutto ciò che concerne l'orario di lavoro, i periodi di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie, nel pieno rispetto della relativa normativa e delle disposizioni previste dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale;
- non sottoporre i propri lavoratori a condizioni, metodi di sorveglianza o condizioni alloggiative (quando previste) degradanti.

7. PRESIDI DI CONTROLLO

Le modalità operative che il Personale della Società è tenuto a osservare per i processi sensibili nell'ambito delle attività di "Selezione, Assunzione e Gestione del Personale" ai fini della prevenzione dei reati di cui al D.lgs. 231/2001 sono di seguito descritte. La Società condanna tramite l'applicazione del Sistema Sanzionatorio i comportamenti difformi alle disposizioni seguenti.

7.1 SELEZIONE E ASSUNZIONE DEL PERSONALE DIPENDENTE

I Responsabili di Filiale e i Responsabili degli Uffici richiedenti risorse umane, eseguono la valutazione delle esigenze della propria unità operativa e inviano le richieste di assunzione alla Direzione Risorse Umane Corporate, dietro autorizzazione del Capo Area e mettendo per conoscenza il Direttore di Divisione, indicandone la motivazione e definendo le competenze necessarie per ricoprire il ruolo.

La Direzione Risorse Umane valuterà se l'assunzione è realmente necessaria in termini organizzativi e di compatibilità con i costi, e se il bisogno non possa essere ugualmente soddisfatto mediante la mobilità interna.

L'autorizzazione della Direzione Risorse Umane è vincolante alla continuazione del processo.

Il Responsabile del Personale, in caso di approvazione, verifica il rispetto delle quantità di lavoratori appartenenti alle categorie protette, facendo eventualmente richiesta alle autorità competenti.

Nel caso in cui il numero dei dipendenti non richieda il ricorso a categorie protette, il Responsabile del Personale avvia la fase di selezione e reclutamento di risorse dall'esterno mediante raccolta dei *curricula* di possibili candidati rispondenti alle caratteristiche richieste.

La selezione del Personale avviene attraverso procedure di autocandidatura dei lavoratori per il tramite del portale *web* ovvero consegna di *curricula*. All'atto della recezione delle predette

candidature, le stesse vengono archiviate ed eventualmente utilizzate laddove si presenti l'esigenza di completare l'organizzazione aziendale.

Altresì la Società si rivolge a soggetti specializzati ed abilitati per la ricerca e selezione del Personale nonché per la somministrazione cui conferisce esplicito incarico relativamente alle figure di cui necessita.

Nel caso in cui sia necessario assumere Personale "Operativo", i colloqui, inderogabilmente e imprescindibilmente vengono effettuati congiuntamente dal Responsabile di settore e dall'Ufficio Risorse Umane, predisponendo per ciascun candidato l'apposito modulo di valutazione.

Se fra i candidati vi sono candidature in linea con le richieste, la Funzione richiedente darà mandato alla Direzione Risorse Umane Corporate per negoziare inquadramento e retribuzione, in coerenza con i contratti applicati e le politiche retributive in atto in azienda e nel rispetto delle normative nazionali e locali.

Per quanto concerne il reclutamento di "Impiegati" e "Quadri", la Direzione Risorse Umane avvia il processo di individuazione della rosa di candidati ritenuti idonei (da tre a cinque) da sottoporre a un primo colloquio. Il secondo colloquio verrà effettuato, sempre e obbligatoriamente, congiuntamente dalla Funzione richiedente e dall'Ufficio Risorse Umane, predisponendo l'apposito modulo di valutazione. Se si ritiene che nella rosa vi sia una candidatura in linea con le richieste, la Funzione richiedente dà mandato alla Direzione Risorse Umane, previa condivisione, per negoziare inquadramento, retribuzione ed eventuali *benefit* da assegnare in coerenza con le politiche retributive in atto in azienda e nel rispetto delle normative nazionali e locali.

Qualora Rangers S.r.l. dia incarico a una società terza di selezione, quest'ultima seguirà la prima fase del processo fino alla presentazione della rosa di candidati. Il secondo colloquio verrà effettuato congiuntamente dal Responsabile della Filiale e dall'Ufficio Risorse Umane.

Sia nel caso di selezione interna sia nel caso di selezione di soggetti esterni, all'atto dell'avvio della selezione, laddove il candidato sia ritenuto eleggibile a una delle posizioni vacanti, la Società, con apposita "Scheda di Evidenza" da allegare al *curriculum* e archiviare anche in formato elettronico in caso di assunzione, si accerta se vi siano condizioni di: (a) parentela con soggetti già alle dipendenze della società; (b) parentela con soggetti che hanno svolto attività di verifica o ispezione nei precedenti 24 mesi; (c) che l'inoltro della domanda non sia stata preceduta da nessuna richiesta di danaro o altra utilità da parte dipendenti/collaboratori/consulenti o qualunque altro soggetto che abbia avuto relazioni anche indirette con la società nei precedenti 24 mesi; (d) che il candidato non sia un pubblico dipendente con il quale negli ultimi due anni la Società abbia intrattenuto rapporti commerciali o comunque inerenti l'attività dello stesso pubblico dipendente, suoi parenti o affini o persone a egli legate anche da un rapporto di amicizia o di interesse; (e) che il candidato non sia un soggetto che ricopre cariche pubbliche o che svolge incarichi pubblici tali da poterlo porre in una situazione di conflitto di interessi, suoi parenti o affini o persone a egli legate anche da un rapporto di amicizia o di interesse.

Il Responsabile della Filiale riassume quanto emerso in sede di colloquio sui *curricula* dei candidati intervistati e consegna tali documenti (compresa la "Scheda di Evidenza") al Responsabile del Personale. Quest'ultimo condivide con la Direzione Divisione Vigilanza i risultati, il quale decide

per il reclutamento oppure per il rifiuto del candidato. In caso di inserimento in azienda, il Responsabile del Personale inserisce la nuova risorsa sul *software* aziendale.

Il Responsabile del Personale è responsabile dell'archiviazione di tutta la documentazione relativa al processo di ricerca e scelta del Personale, compresa la "Scheda di Evidenza" per la selezione del Personale di cui sopra.

7.1.1 ASSUNZIONE DEL PERSONALE DIPENDENTE STRANIERO

Il datore di lavoro non può impiegare lavoratori stranieri privi di permesso di soggiorno o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale.

In caso di assunzioni di dipendenti stranieri:

1. Il Responsabile del Personale verifica che, il candidato straniero, sia in possesso di un regolare permesso di soggiorno;
2. L'ufficio del personale è tenuto a farsi consegnare preventivamente copia del permesso di soggiorno.
3. In seguito all'assunzione del lavoratore straniero:

    - l'ufficio del personale prende preventivamente atto del permesso di soggiorno come sopra indicato;
    - l'ufficio del personale è tenuto a monitorare la valenza del permesso di soggiorno in corso di rapporto di lavoro, richiedendo al lavoratore straniero prova della richiesta di rinnovo nei termini di legge e comunque prima della scadenza del permesso di soggiorno stesso;
    - l'ufficio del personale comunica immediatamente al datore di lavoro l'eventuale omessa richiesta di rinnovo del permesso di soggiorno nei termini di legge da parte del lavoratore straniero alle sue dipendenze;
    - in ogni caso, il lavoratore straniero è tenuto a comunicare immediatamente al datore di lavoro l'intervenuta scadenza, revoca o annullamento del permesso di soggiorno; a seguito di tale eventuale comunicazione, il datore di lavoro provvede nei termini di legge.

7.1.2 INFORMAZIONE E FORMAZIONE DEL NEOASSUNTO

La comunicazione e la formazione costituiscono strumenti essenziali al fine di un'efficace implementazione e diffusione del Modello Organizzativo e del relativo Codice Etico.

La Direzione Risorse Umane garantisce una corretta conoscenza dei principi e delle regole di condotta adottati dalla società sia alle risorse già presenti sia a quelle future, con differente grado di approfondimento in relazione al loro diverso livello di coinvolgimento nei processi operativi considerati sensibili e rilevanti.

L'Ufficio del personale cura e promuove adeguate iniziative di diffusione in caso di revisione del Modello Organizzativo. L'attività di formazione è finalizzata a promuovere la conoscenza della normativa di cui al D.Lgs. 231/01, delle sue conseguenze operative, nonché dei contenuti e dei principi su cui si basa il Modello Organizzativo e il relativo Codice Etico fra tutti i dipendenti che, pertanto, sono tenuti a conoscerli, osservarli e rispettarli, contribuendo alla loro attuazione. L'attività di formazione, eventualmente anche tramite corsi *on line*, è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della società.

Al momento dell'assunzione, la società, promuove la conoscenza del Modello Organizzativo e del Codice Etico. Ai neoassunti viene consegnata un'informativa con riferimento all'applicazione della normativa di cui al Decreto Legislativo 231/2001 nell'ambito della società, in particolare:

1. Una volta accettata, il Responsabile della Direzione Risorse Umane firma la lettera di assunzione predisposta dalla amministrazione di concerto con il professionista/ente incaricato dell'amministrazione del personale, e comunica al neo assunto l'inquadramento giuridico contrattuale e le relative spettanze retributive.
2. Con l'assunzione, il neo assunto viene reso edotto circa il modello organizzativo implementato in ottemperanza alla normativa ex d.lgs. n. 231/2001, anche in relazione agli obblighi relativi.
3. Sono consegnati all'assunto il codice di condotta (etico) e le procedure previste dal Modello della società e viene raccolta la dichiarazione di accettazione dell'assunto, avendo particolare riguardo a quanto previsto in merito all'uso dei sistemi informatici ed ai controlli relativi.
4. L'assunto è quindi sottoposto ai percorsi di informazione, formazione ed addestramento previsti dalle norme in vigore materia di sicurezza nei luoghi di lavoro.
5. A seguito dell'assunzione sono altresì assegnati il profilo, l'identificativo (ID) e la password di accesso ai sistemi informatici del caso. Si applica la procedura "Uso dei sistemi informatici".

7.1.3 CESSAZIONEDEL RAPPORTO DI LAVORO

Fermo restando quanto previsto dai contratti collettivi in materia di conclusione/cessazione del rapporto di lavoro, l'Ufficio del Personale comunica al Responsabile IT l'avvenuta cessazione del rapporto di lavoro, inibendo i servizi attivati al momento dell'assunzione (email/password aziendale).

Contestualmente alla cessazione del rapporto di lavoro, l'Ufficio Risorse Umane è tenuto a richiedere e ottenere tutto il materiale elettronico che gli sia stato reso disponibile ed ogni altro bene fornito dalla Società (es. divisa, automobile), entro la data di cessazione effettiva del rapporto di lavoro.

Dell'avvenuta restituzione, è rilasciata da parte dell'Ufficio Risorse Umane al dipendente, apposita ricevuta.

7.2 SELEZIONE E ASSUNZIONE DI GUARDIE PARTICOLARI GIURATE

All'atto dell'assunzione di nuove risorse umane, Rangers S.r.l. valuta i candidati a seconda che le

mansioni da svolgere prevedano o meno il possesso del decreto di nomina a Guardia Particolare Giurata (G.P.G.). Nel primo caso, l'aspirante dovrà ottenere il decreto di nomina a guardia particolare e il porto d'armi, nonché altri requisiti ritenuti necessari dalla Società. Nel secondo caso, non è necessario ottenere il porto d'armi.

La veridicità dei documenti è verificata dalla Direzione Risorse Umane.

Per tutte le G.P.G. è prevista, a cura della Direzione Risorse Umane, una formazione specifica relativa alla gestione delle situazioni di pericolo e alla normativa sulla difesa personale e dei beni articolata secondo quanto prescritto dai regolamenti vigenti.

7.3 SICUREZZA DEI LAVORATORI

Per un'effettiva prevenzione dai rischi sui luoghi di lavoro, e in conformità anche agli adempimenti prescritti dal D.lgs. 81/2008, è fatta espressa richiesta ai soggetti aziendali, (es. il Datore di Lavoro) e agli Uffici aziendali individuati a vario titolo coinvolti nella gestione del sistema sicurezza, di svolgere i compiti loro attribuiti in tale materia, nel rispetto delle procedure aziendali esistenti, senza mai esporre i lavoratori a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni generali di lavoro, avendo cura di informare e formare il Personale che, nello svolgimento delle proprie attività, sia esposto a rischi connessi alla sicurezza, promuovendo la cooperazione e il coordinamento attraverso la elaborazione del Documento di Valutazione dei Rischi (DUVRI) che indichi le misure adottate per eliminare o ridurre al minimo i rischi derivanti dalle possibili interferenze tra l'attività dei propri lavoratori e quella dei lavoratori alle dipendenze di altra società interessata al medesimo lavoro.

A tal proposito, la Direzione Risorse Umane unitamente al RSGSL archiviano tempestivamente tutta la documentazione rilevante in materia di sicurezza e salute sul lavoro, in particolare quella relativa a visite mediche, infortuni e malattie professionali. La Direzione Risorse Umane archivia altresì la documentazione relativa alla formazione obbligatoria prevista dal D.lgs. 81/2008.

Qualora il Medico competente, a seguito degli accertamenti sanitari, esprima un giudizio sull'inidoneità parziale o temporanea o totale del lavoratore, informa per iscritto il Datore di Lavoro e il suo delegato, i quali, di concerto con la Direzione Risorse Umane, adottano tempestivamente le decisioni necessarie a evitare che i lavoratori siano esposti a situazioni di pericolo.

Ogni dipendente è tenuto a segnalare al proprio superiore gerarchico e/o al Datore di Lavoro e al suo delegato, ogni comportamento difforme da quello sopra previsto.

Si rinvia al Protocollo "Gestione degli adempimenti previsti in materia di sicurezza, salute sul lavoro e ambiente".

7.4 GESTIONE DELLE NOTE DI SPESA E DELLE SPESE DI RAPPRESENTANZA

La Società rimborsa ai propri dipendenti le spese effettive, ragionevoli, opportunamente documentate e necessarie, sostenute per ragioni di servizio in occasione di viaggi o spostamenti al di fuori della sede abituale di lavoro.

È inoltre previsto il mero rimborso delle spese di rappresentanza sostenute nel corso di riunioni o incontri d'affari con soggetti esterni alla Società, purché adeguatamente documentate e autorizzate dal Responsabile di Funzione.

La liquidazione delle note spese deve essere autorizzata per iscritto, previo controllo, ovvero in casi di necessità e/o urgenza ratificata subito dopo l'impegno di spesa.

La gestione dei rimborsi spese deve avvenire in accordo alla normativa, anche fiscale, applicabile.

Le spese di trasferta rimborsabili devono essere direttamente riferibili a incarichi di servizio ed essere controllate in base a criteri di economicità e di massima trasparenza.

È vietata la concessione di rimborsi spese a soggetti non dipendenti della Società, qualora non previsto dal contratto/lettera d'incarico (es.: consulenti).

È comunque vietata la concessione di rimborsi spese a favore di soggetti della Pubblica Amministrazione.

Per le modalità di rimborso delle note spese si rinvia alla *policy* aziendale "Viaggi e trasferte". Eventuali anomalie sono comunicate all'OdV.

7.5 GESTIONE DELLA SEGNALAZIONE DI SINISTRI

La Direzione Risorse Umane, una volta ricevuta la segnalazione di sinistro a opera del Responsabile di Filiale ovvero dell'Ufficio Automezzi, analizzate la documentazione e le relazioni compilate dagli operativi come prescritto dalla relativa *Policy* aziendale, verifica l'entità e la gravità del sinistro e la sussistenza di profili di responsabilità di natura disciplinare in capo al lavoratore o ai lavoratori coinvolti. Qualora emergesse, anche solo nell'ambito di un concorso di colpe con terzi, una fonte di responsabilità disciplinare in capo al lavoratore/lavoratori interessati, appronta la relativa lettera di contestazione disciplinare *ex* art. 7 legge n. 300/1970. Il medesimo Ufficio, qualora il fatto posto a base del sinistro dovesse essere di entità/gravità tale da generare eventuali contenziosi, trasmette a sua volta la medesima documentazione al competente Ufficio Legale il quale dovrà aprire anch'esso un fascicolo per effettuare le valutazioni del caso in termini di gestione legale del sinistro, sia attivo che passivo, eventualmente coinvolgendo l'istituto assicurativo.

7.6 MODIFICA DEGLI ORGANIGRAMMI

Qualora sorga l'esigenza di modificare gli organigrammi aziendali creando una nuova posizione o assegnando una posizione esistente - scoperta ovvero ricoperta da un soggetto ritenuto inadeguato – a un soggetto diverso che abbia i requisiti necessari a ricoprirla, l'Ufficio Risorse Umane si interfaccia con gli Uffici interessati alla modifica dell'organigramma, formulando una proposta di revisione e selezionando i soggetti idonei cui assegnare i ruoli coinvolti. La proposta di revisione dell'organigramma è condivisa dalla Direzione Risorse Umane con il Consiglio di Amministrazione, che approva la modifica.

La Direzione Risorse Umane trasmette al Responsabile dell'Organizzazione Aziendale Corporate una relazione sulla scelta adottata nonché la bozza di comunicazione organizzativa che il

Responsabile dell'Organizzazione Aziendale dovrà sottoscrivere e veicolare in Azienda attraverso gli strumenti previsti.

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Al fine di verificare il processo in oggetto, i Responsabili delle Funzioni/Uffici interessati e, più in generale, i soggetti muniti di poteri in base al sistema di deleghe e procure sono tenuti a inviare, con periodicità definita dall'Organismo di Vigilanza, adeguati flussi informativi.

Conformemente a quanto stabilito nella Parte Generale, fermo restando il suo potere discrezionale di attivarsi con specifici controlli di propria iniziativa o a seguito della segnalazione ricevute, l'OdV effettua periodicamente controlli a campione sulle attività di "Selezione, Assunzione e Gestione del Personale", e comunque su ogni attività sensibile individuata nel presente Protocollo, diretti a verificarne l'applicazione in conformità a quanto sopra previsto.

9. CONSERVAZIONE DELLA DOCUMENTAZIONE

I Responsabili delle Funzioni/Uffici coinvolti nei processi sensibili individuati nel presente protocollo operativo sono responsabili, ciascuno per la parte di propria competenza, della conservazione della documentazione, nel rispetto dei termini di legge, al fine di garantire la tracciabilità delle operazioni aziendali. La documentazione è, inoltre, messa a disposizione, su richiesta, del Consiglio di Amministrazione, del Sindaco Unico e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001
RELATIVO AL PROCESSO
GESTIONE ED ESECUZIONE DEI SERVIZI DI VIGILANZA E TRASPORTO

INDICE

1. FINALITÀ 2

2. ILSISTEMADEICONTROLLI 2

2.1. STANDARDDI CONTROLLO GENERALI 2
2.2. STANDARD DI CONTROLLO SPECIFICI 3

3. AMBITO DI APPLICAZIONE 4

4. NORMATIVA DI RIFERIMENTO 4

5. REATI ASTRATTAMENTE PERPETRABILI 5

6. REGOLE GENERALI DI COMPORTAMENTO 13

7. PRESIDI DI CONTROLLO 15

7.1 GESTIONE DEI SERVIZI EROGATI 15
7.2INSTALLAZIONE DI APPARECCHIATURE DI VIDEOREGISTRAZIONE NELL'AMBITO DEI SERVIZI DI VIGILANZA EROGATI 18

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA 18

9. CONSERVAZIONE DELLA DOCUMENTAZIONE 19

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il Personale deve attenersi nell'ambito del processo di "**Gestione ed esecuzione dei servizi di vigilanza e trasporto".**

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice Etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società, nelle procedure e istruzioni operative e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi Sociali, i Dipendenti, i Collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;
- Fornire all'OdV e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei Dipendenti – in via diretta – dei Collaboratori Esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione-di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da - considerati individualmente o collettivamente - integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, nonché delle "*best practice*", prevede con riferimento alle Aree e alle Attività Sensibili individuate:

- *Standard di controllo "generali"*, applicabili a tutte le Attività Sensibili;
- *Standard di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

2.1. STANDARDDI CONTROLLO GENERALI

Gli *standard* di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:

- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e

autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;

- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa- Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

2.2. STANDARD DI CONTROLLO SPECIFICI

Sulla base degli *standard* di controllo generali sopra riportati, gli *standard* di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;

- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema delle deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

3. AMBITO DI APPLICAZIONE

Il presente Protocollo si applica a Rangers S.r.l.(di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 ed è rivolto a tutti i soggetti aziendali coinvolti, a vario titolo, nel processo di Gestione ed esecuzione dei servizi di vigilanza e trasporto. Concerne, in particolare, tutte quelle funzioni/uffici interessati e coinvolti nei seguenti processi:

- Attività di trasporto;
- Attività di vigilanza presso clienti pubblici e privati;
- Negoziazione e stipulazione dei contratti;
- Installazione di apparecchiature di videoregistrazione e videosorveglianza.

Le Funzioni aziendali coinvolte a qualsiasi titolo nella presente procedura sono:

- Direzione Vigilanza;
- Area tecnica;
- Direzione Commerciale;
- Responsabile Commerciale;
- Direzione Operazioni;
- Responsabile Operazioni;
- Responsabile Centrale Operativa;
- Responsabile Sviluppo Operativo;
- Responsabili di Filiale;
- Direzione Sistemi di sicurezza e innovazione;
- Responsabile Sistemi di sicurezza e innovazione:
- Responsabile di conformità per la prevenzione della corruzione (RAC).

4. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30"*;
- Regio Decreto 18 giugno 1931, n. 773, "*Testo unico delle Leggi di Pubblica Sicurezza*";
- R.D.L. 26/9/1935 n. 1952 convertito in Legge 508/36 "*Disciplina del servizio delle Guardie Particolari Giurate"*.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l..;
- Codice Etico del Gruppo Battistolli;
- Manuale Antiriciclaggio;
- Procedure e istruzioni operative;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Sistema di gestione di prevenzione della corruzione (UNI ISO 37001:2016);
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

5. REATI ASTRATTAMENTE PERPETRABILI

I reati presupposto (nella forma consumata o tentata) di cui al D.lgs. 231/01 da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati:

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25):**
  - Truffa in danno dello Stato o di un ente pubblico (art. 640, comma 2, n. 1, c.p.)

Il reato di concussione si caratterizza per l'utilizzo indebito da parte del funzionario pubblico dei propri poteri, al fine di costringere il soggetto passivo a riconoscere al funzionario o ad un terzo soggetto un vantaggio di natura economica o personale. Si ha abuso dei poteri quando gli stessi siano esercitati fuori dei casi previsti da leggi, regolamenti e istruzioni di servizio o senza le forme prescritte, ovvero quando detti poteri, pur rientrando tra quelli attribuiti al pubblico ufficiale, vengano utilizzati per il raggiungimento di scopi illeciti.

  - Corruzione (artt. 318, 319, 320, 322-*bis* c.p.)

Il reato di corruzione consiste in un accordo fra un pubblico funzionario e un privato, in forza del quale il primo accetta dal secondo un compenso che non gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria). Nella corruzione il pubblico ufficiale ed il privato sono in posizione paritaria, diversamente dalla concussione che invece presuppone lo sfruttamento da parte del funzionario della propria posizione di superiorità alla quale corrisponde una situazione di soggezione nel privato. La fattispecie prevista dall'art. 319 c.p., connotata come quella di cui all'art. 318 c.p. da un rapporto paritetico tra pubblico ufficiale/ incaricato di un pubblico servizio-corrotto e privato-corruttore, se ne differenzia in virtù del fatto che l'atto richiesto al pubblico ufficiale o all'incaricato di un pubblico servizio a fronte della dazione o della promessa di denaro o di altra utilità, risulta contrario ai doveri d'ufficio. In particolare la condotta può concretizzarsi in una omissione o in un ritardo nel compimento di un atto di ufficio ovvero nel compimento di un atto contrario ai doveri di ufficio.

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

Il reato è configurabile solo ove l'offerta del privato o la richiesta del pubblico funzionario non vengano accolte dal destinatario. Tuttavia, ove il rifiuto non sia stato immediato e siano incorse trattative poi non sfociate in un accordo, si ritiene configurabile un tentativo di corruzione del quale rispondono entrambi i soggetti. Nell'istigazione alla corruzione passiva la condotta consiste nell'offrire o nel promettere denaro o altra utilità non dovuti al funzionario. L'offerta o la promessa deve essere seria e concreta ed idonea alla realizzazione dello scopo, tale cioè da indurre il destinatario a compiere o a ritardare un atto dell'ufficio o del servizio ovvero a fare un atto contrario a detti doveri. L'idoneità dell'offerta va valutata con un giudizio "ex ante" che tenga conto dell'entità del compenso, delle qualità personali del destinatario e della sua posizione economica e di ogni altra connotazione del caso concreto.

- **Reati in materia di ricettazione, riciclaggio e impiego di denaro di provenienza illecita, introdotti dal d.lgs. 231/2007 (art. 25-*octies*):**
  - Ricettazione (art. 648 c.p.)

L'incipit della norma, in relazione al soggetto attivo, esclude che possa essere autore della ricettazione colui che ha commesso il reato da cui i beni provengono. Dunque chi commissiona il delitto presupposto concorre nella sua realizzazione come istigatore ed è punibile a tale titolo, mentre la successiva condotta di ricezione rileva come mero post factum non punibile. L'oggetto materiale è costituito da denaro o cose provenienti da delitto. La giurisprudenza vi comprende i servizi, l'energia o programmi di *know how*, mentre si divide riguardo gli immobili. Infine, riguardo ai rapporti con le figure concorrenti, si può tendenzialmente affermare che la ricettazione è destinata a lasciare spazio alle previsioni che incriminano specificamente la ricezione di un determinato bene di origine illecita. Ad esempio, in applicazione del principio di specialità *ex* art. 15 c.p., gli artt. 453, n. 3/4 e 455 c.p., che sanzionano chi acquista, riceve o detiene monete contraffate o alterate al fine di metterle in circolazione, sono destinati a prevalere sull'art. 648 c.p.

  - Riciclaggio (art. 648-*bis* c.p.)

Anche ai fini della configurabilità del reato di riciclaggio è necessario che sia in precedenza consumata altra fattispecie criminale. Più precisamente, affinché vi sia un provento illecito da riciclare – sia esso denaro o altro bene o utilità – è imprescindibile il fatto che un reato, per l'appunto presupposto sia stato commesso. Il riciclaggio consiste, quindi, nelle attività volte a dissimulare l'origine illecita dei proventi criminali ed a creare l'apparenza che la loro origine sia lecita.

  - Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.)

Chi impiega denaro di provenienza delittuosa, direttamente in un'attività economica o finanziaria, così ripulendolo, risponde non del reato di riciclaggio, ma di quello punito dall'art. 648-ter c.p. appunto «Impiego di denaro, beni o utilità di provenienza illecita». In quest'ultimo, infatti, è "assorbita" la precedente attività di sostituzione o di ricezione. Invece, se taluno sostituisce denaro di provenienza illecita con altro denaro o altre unità e, poi, impieghi i proventi derivanti da tale opera di ripulitura in attività economiche o finanziarie, risponde del solo reato di riciclaggio (art. 648 bis c.p.) con esclusione del 648-ter c.p.

Al fine di distinguere la fattispecie rispetto agli omogenei reati di riciclaggio (in senso stretto) e ricettazione la giurisprudenza ha chiarito che il delitto di cui all'art. 648 cod. pen. richiede una generica finalità di profitto, quello di cui all'art. 648 bis cod. pen. lo scopo ulteriore di far perdere le tracce dell'origine illecita, quello, infine, di cui all'art. 648 ter cod. pen. che tale scopo sia perseguito mediante l'impiego delle risorse in attività economiche o finanziarie. Cassazione Penale, Sez. 2, Sentenza n. 33076 del 14/07/2016 Cc. (dep. 28/07/2016) Rv. 267692 - 01

Esempio: la giurisprudenza ha dichiarato la sussistenza di questa fattispecie in un caso in cui la società aveva utilizzato capitali di provenienza illecita, riconducibili al gestore del patrimonio di un sodalizio di stampo mafioso, per coprire crisi di liquidità, onorare gli impegni assunti con le banche e i fornitori, ed incrementare l'attività aziendale. Cassazione penale, Sez. I, sentenza n. 2737 del 26 gennaio 2011.

Al fine di contrastare la realizzazione della fattispecie è prevista, quale regola generale di comportamento, la necessità di "identificare la clientela e prevedere la raccolta delle informazioni necessarie alla valutazione del rischio riciclaggio per tutti i rapporti continuativi nonché per i clienti che eseguono operazioni occasionali di importo pari o superiori a € 15.000" nonché una verifica periodica delle condizioni del cliente in itinere.

  - Autoriciclaggio (art. 648-*ter* 1 c.p.)

Il delitto di riciclaggio, così come formulato dall'art. 648- bis c.p., punisce chi ricicla denaro, beni o altre utilità provenienti da un delitto non colposo commesso da un altro soggetto, mentre nessuna sanzione era prevista per chi ricicla in prima persona , cioè sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo da egli commesso (o che ha concorso a commettere), ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. L'introduzione del reato di autoriciclaggio è stata necessaria per colmare questa lacuna nel nostro ordinamento. Il delitto di autoriciclaggio, peraltro, prevede pene diverse a seconda della gravità del delitto presupposto e con previsione della non punibilità delle condotte nelle quali il denaro, i beni o le altre utilità vengono destinati «alla mera utilizzazione o al godimento personale».

- **Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, introdotti dal D.Lgs. 184/2021 e modificati dalla L. n. 137/2023 (art. 25 octies I):**

  - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter, co. I c.p.).

Il delitto di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, così come formulato dall'art. 493 ter, co. I c.p., punisce chi indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti. La norma contempla, altresì, l'ipotesi del soggetto che falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. La novella del legislatore estende il campo della condotta, contemplando ogni strumento di pagamento diverso dal contante che sia idoneo ad abilitare al prelievo del denaro o all'acquisto di beni o prestazione di servizi o comunque rappresenti uno strumento di pagamento diverso dal contante.

  - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater, co. I c.p.).

La norma contempla l'ipotesi in cui, salvo che il fatto costituisca più grave reato, il soggetto che, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

  - Frode informatica (640 ter, co. I c.p.).

Il delitto di frode informatica, così come formulato dall'art. 640 ter, co. I c.p., punisce chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. La norma prevede, peraltro, pene diverse a seconda che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale o sia commesso con abuso della qualità di operatore del sistema dall'ipotesi, più grave, in cui il fatto sia commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

- **Reati transnazionali, introdotti dalla Legge 146/2006 (modificati dalla legge 94/2009), in particolare:**
  - Associazione per delinquere (art. 416 c.p.);

I delitti associativi in generale hanno carattere plurisoggettivo, ossia richiedono la partecipazione di almeno tre persone. La partecipazione può essere anche di secondaria importanza, purché il contributo sia apprezzabile, concreto e dotato di effettiva stabilità. Ai fini della configurabilità del delitto di associazione per delinquere, è necessaria la predisposizione di un'organizzazione strutturale, sia pure minima, di uomini e mezzi, funzionale alla realizzazione di una serie indeterminata di delitti, nella consapevolezza, da parte dei singoli associati, di far parte di un sodalizio durevole e di essere disponibili ad operare per l'attuazione del programma criminoso comune. In altre parole, l'art. 416 c.p. punisce coloro che promuovono, costituiscono o organizzano l'associazione allo scopo di commettere più delitti. Anche il solo fatto di partecipare all'associazione costituisce reato.

  - Associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.);

La prima differenza da evidenziare risiede nella diversità di scopo delle associazioni previste all'art. 416 e all'art. 416 bis. L'associazione per delinquere ex art. 416 c.p. agevola la commissione dei c.d. reati–fine, essi solo fonte dei possibili redditi o proventi illeciti, per la cui produzione è allora indispensabile la consumazione di un autonomo e diverso reato; invece, l'associazione di tipo mafioso si qualifica per la possibilità di produrre per sé reddito o proventi illeciti, come se caratterizzata da una presunzione assoluta di produzione illecita; sicché è l'associazione in sé a rendere le attività (acquisite o gestite) illegali, perché perseguite e realizzate con gli strumenti dell'omertà, dell'intimidazione e della violenza. Ancora, se l'associazione a delinquere "semplice" postula necessariamente la commissione di un certo reato-fine (nel senso che verrà costituita in funzione della sua commissione e realizzazione), l'associazione di tipo mafioso può anche, in ipotesi, non essere finalizzata alla commissione di delitti, ben potendo avere come scopo il compimento di attività lecite, le quali, però, degradano ad illecite per il solo fatto di esser state compiute dall'associazione medesima. La tipicità del modello associativo mafioso risiede, quindi, nella modalità attraverso cui l'associazione si manifesta concretamente e non negli scopi che si intendono perseguire. Tali scopi abbracciano solo genericamente "i delitti" comprendendo una varietà indeterminata di possibili tipologie di condotte che possono anche essere costituite da attività in sé lecite. La tipicità dello schema e della struttura del reato di associazione per delinquere di tipo mafioso va dunque colta nelle modalità in cui esso si manifesta in concreto e non nelle finalità che l'associazione persegue o intende perseguire.

  - Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (DPR 43/1973, art. 29-*quater*);

Tale reato è un'ipotesi particolare del reato associativo di cui all'art. 416 c.p. con cui astrattamente può anche concorrere. L'evento, nel reato di contrabbando, si compendia nell'esposizione a pericolo del bene giuridico tutelato - il diritto dello Stato a percepire il tributo - per effetto di un'attività posta in essere dall'agente volontariamente con il consapevole intento di eludere il pagamento di quest'ultimo.

  - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (DPR 309/1990, art. 74);

Il reato in questione è un'ipotesi particolare del reato associativo di cui all'art. 416 c.p. e si differenzia solo per la speciale natura dei delitti da commettere, che rientrano nelle sue finalità e con cui astrattamente può anche concorrere. L'associazione per delinquere, finalizzata al traffico di sostanze stupefacenti, è realizzata sia dall'unione di più persone che operano, anche in via soltanto parallela, per la realizzazione di profitti con lo spaccio della droga, sia dal vincolo che lega, anche oggettivamente, l'importatore-acquirente, che si adopera per rifornire il mercato, in via continuativa, con la rete di piccoli spacciatori, purché tutti i soggetti abbiano la consapevolezza di agire nell'ambito di una organizzazione, nella quale l'attività dei singoli si integra strumentalmente per la finalità perseguita e purché l'acquirente-rivenditore sia stabilmente disponibile, inoltre, a ricevere le sostanze stupefacenti con tale continuità da proiettare il singolo atto negoziale oltre la sfera individuale, come elemento della complessiva ed articolata struttura organizzativa. Per la realizzazione del reato in questione non si richiede una vera e propria organizzazione, bastando la concordanza e la convergenza di condotte significativamente integrate in un contesto di stabile e continuativa disponibilità, così da costituire un punto di riferimento e di sicura affidabilità nel progetto di massima d'intermediazione nel concordato traffico di stupefacenti

- Disposizioni contro le immigrazioni clandestine (D.lgs. 286/1998 art. 12);

Il reato in questione non richiede per il suo perfezionamento che l'ingresso illegale sia effettivamente avvenuto, trattandosi di un reato a condotta libera ed a consumazione anticipata. Il reato è pertanto integrato anche qualora venga soltanto offerto un contributo preventivo diretto a favorire l'ingresso clandestino di stranieri nel territorio dello Stato. Il reato di favoreggiamento dell'illegale presenza di stranieri extracomunitari nel territorio dello Stato di cui al comma 5 non è configurabile per il solo fatto dell'assunzione al lavoro di immigrati clandestini, occorrendo anche la finalità di ingiusto profitto, riconoscibile soltanto quando si esuli dall'ambito del normale rapporto sinallagmatico di prestazione d'opera.

- Favoreggiamento personale (art. 378 c.p.).

Il favoreggiamento personale è un reato di pericolo e, nella maggioranza delle ipotesi, istantaneo. La condotta tipica è rappresentata da ogni comportamento, anche negativo, sufficiente a depistare o escludere le indagini di polizia non richiedendo la norma l'effettività materiale dell'azione. Oggetto dell'attività penalmente rilevante è il comportamento, cosciente e volontario, posto in essere dal reo destinato all'intralcio dell'attività investigativa e finalizzato all'aiuto dell'autore materiale di un altro reato. Integra la fattispecie di reato in oggetto anche colui il quale presti il suo aiuto al colpevole, al fine di sottrarlo alle indagini, quando queste non siano ancora iniziate. La definizione di "aiuto" comprende non solo le condotte finalizzate alla creazione di barriere ostative alle indagini ma anche quelle di natura puramente omissiva; dunque comportamenti quali il silenzio, la reticenza e la mendacità sull'identità del colpevole sono idonei ad integrare il reato in oggetto.

- **Reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro, introdotti dalla Legge 123/2007(art. 25-*septies*):**
  - Omicidio colposo (art. 589 c.p.);

La giurisprudenza maggioritaria accoglie l'interpretazione che ritiene di dover ricollegare, nel caso di reati presupposto colposi, all'interesse o vantaggio dell'ente, non il reato nel suo insieme di condotta ed evento, ma solo la condotta penalmente rilevante. Tale orientamento giurisprudenziale si fonda sulla semplice constatazione che, nel caso di omicidio colposo o lesioni personali colpose in violazione delle norme sulla sicurezza dei lavoratori, l'evento lesivo (ovvero la morte o la lesione) non potrebbe mai rispondere ad un interesse o vantaggio dell'ente, e pertanto l'art. 25-septies non potrebbe mai trovare applicazione. Alla luce di tale interpretazione si comprende chiaramente perché, nel caso di reati colposi, l'unico criterio che può venire in gioco è quello del vantaggio, rappresentato dai risparmi di spesa derivanti, per esempio, dalla mancata adozione delle necessarie misure antiinfortunistiche. L'interesse, infatti, letto come intenzione dell'agente di favorire l'ente, si scontra inevitabilmente con l'elemento psicologico della colpa.

- Lesioni personali colpose, gravi o gravissime (art. 590 c.p.).

La Corte di Cassazione, con la sentenza n. 8861/2013, è intervenuta nuovamente sul tema della responsabilità del datore di lavoro per lesioni subite dal dipendente che, durante una trapanazione all'interno di un container, era colpito all'occhio da una scheggia di metallo. Il Supremo Collegio ha condiviso la tesi del giudice di merito secondo cui non sarebbe sussistita la responsabilità del datore di lavoro poichè quest'ultimo «aveva provveduto a fornire, a mezzo dei suoi preposti, i necessari mezzi di protezione (kit contenente, tra gli altri, guanti ed occhiali) ad impartire istruzioni sull'uso degli stessi ed a vigilare sul rispetto delle istruzioni impartite e sull'uso degli occhiali di protezione durante la lavorazione e che, rispetto al puntuale assolvimento di tutti questi obblighi, la condotta del lavoratore aveva assunto il carattere dell'assoluta imprevedibilità». Tale giurisprudenza si trova anche nella sentenza n. 6363/2013, là dove - in conformità con i precedenti giurisprudenziali della Corte di Cassazione - la responsabilità del datore di lavoro non è stata esclusa neppure dalla colpa del lavoratore, poichè la condotta di questi non ha assunto i caratteri dell'"abnormità", risultando eccezionale ed imprevedibile.

- **Delitti di criminalità organizzata, introdotti dalla Legge 94/2009 (art. 24-*ter*), in particolare:**
  - Delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2 comma 3, della legge 18 aprile 1975, n. 110 (art. 407, comma 2, lett. a), numero 5) c.p.p.).

Sono considerate armi comuni da sparo quelle denominate "da bersaglio da sala" o a emissione di gas, strumenti lanciarazzi e le armi ad aria compressa, sia lunghe che corte, escluse quelle destinate alla pesca e quelle per le quali la commissione consultiva di cui al successivo art. 6 escluda, in relazione alle caratteristiche proprie delle stesse, l'attitudine a recare offesa alla persona.

- **Delitti informatici e trattamento illecito di dati, introdotti dalla Legge 48/2008 (art. 24-*bis*):**
  - Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.);

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Cass. 3067/1999). Il sistema informatico, dovendo svolgere una funzione - mediante tecnologie informatiche - è dunque tale se gestisce o elabora dati, mentre tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è "sistema informatico".
Dirimente ai fini della configurabilità del reato è la presenza o meno delle cd. misure di sicurezza nel sistema informatico / telematico. L'apposizione di siffatte misure protettive del sistema informatico o telematico costituisce, infatti, l'estrinsecazione della *voluntasexcludendi*manifestata dal titolare del relativo *ius*.

  - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.);
  - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.);

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.);

Tale norma mira a impedire l'intercettazione fraudolenta, ravvisabile ogniqualvolta l'agente prenda conoscenza delle comunicazioni in maniera occulta e senza essere legittimato.

- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.);

Tale norma è volta a sanzionare la semplice predisposizione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.);

L'art. 635-bis non si limita ad ampliare ed integrare la norma sul danneggiamento (art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispone altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilo sanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali: il sistema informatico o telematico, ovvero il supporto materiale delle informazioni. Il danneggiamento si può attuare nella distruzione e nel deterioramento e nell'inservibilità totale o parziale.

- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.);
- Danneggiamento di sistemi informatici e telematici (art. 635- *quater* c.p.);

Oltre ad essere realizzabile mediante le condotte indicate nell'art. 635-bis, è prevista anche la punibilità di chi introduce o trasmette dati, informazioni o programmi. Tale previsione si è resa necessaria per punire specificamente i danneggiamenti realizzabili anche a distanza mediante *malware* introdotti o fatti circolare in rete.

- Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-*quinquies* c.p.).

Si è scelto volutamente di codificare autonomamente tutti quei comportamenti delittuosi commessi ai danni di "Enti pubblici o, ad essi pertinenti, o comunque di pubblica utilità". La semplice "condotta" diretta alla commissione del reato, con eccezione di quanto previsto dall'art. 635-bis, è di per ségià punibile non essendo necessario provare che il comportamento del reo raggiunga lo scopo prefissato, venendo quest'ultimo ad influire solo sulla quantificazione della pena. Il legislatore anticipa la soglia di punibilità al fine di meglio sottolineare e quindi sanzionare tutta una serie di comportamenti illeciti riscontrati in questi anni.

- **Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, introdotti dalla Legge 409/2001 e modificati con Legge 99/2009 (art. 25-*bis*):**
  - Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
  - Alterazione di monete (art. 454 c.p.);

Per "contraffazione" generalmente s'intende la formazione integrale della cosa imitata, con notevole grado di fedeltà. Caratteristica principale della contraffazione è, pertanto, l'imitazione della cosa reale, l'apparenza di genuinità. L'alterazione ha, invece, come presupposto l'esistenza di una moneta genuina e la sua circolazione legale costante e consiste, attraverso la manomissione, in una modificazione della sostanza o delle caratteristiche formali della moneta, tale da alterarne il valore. Sia nella fattispecie di cui all'art. 453 c.p. che in quella di cui all'art. 454 c.p. il legislatore ha inteso punire sia il soggetto che pone in essere la contraffazione o l'alterazione; sia colui che, in concerto con chi abbia proceduto alla contraffazione o alterazione o con un suo intermediario, metta in circolazione in qualsiasi modo le monete così contraffatte o alterate; sia, infine, colui che, al fine di metterle in circolazione, le procuri presso il soggetto che le ha contraffatte o alterate o presso un suo intermediario.

- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);

La Corte di Cassazione ha affermato che la fattispecie criminosa di cui all'art. 455 c.p. si sostanzia in una vera e propria forma di ricettazione. L'elemento psicologico del reato in questione consiste nella finalità di mettere in circolazione la falsa moneta, ricevuta in mala fede, a tanto consegue che, da un lato, non può ravvisarsi *dolus "in re ipsa"*, dall'altro, esso può essere desunto solo da elementi sintomatici, gravi e convergenti, idonei a rappresentare, in modo inequivoco, l'intenzione di mettere in circolazione la banconota.
Tra gli elementi da valorizzare, in particolare, vi sono: a) il numero ed il valore delle false monete detenute; b) il tempo intercorso tra la ricezione e la spendita delle stesse; c) lo scopo della conservazione e della mancata consegna all'autorità.

- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Uso di valori bollati contraffatti o alterati (art. 464, commi 1 e 2, c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (474 c.p.).

La tutela prevista per le fattispecie di cui agli artt. 473 e 474 c.p. deve ritenersi limitata, secondo le interpretazioni giurisprudenziali ai soli marchi registrati. La registrazione rappresenterebbe, pertanto, il presupposto della condotta. L'interesse giuridico tutelato dalla norma dell'art. 473 c.p. (in piena coincidenza con quello dell'art. 474 c.p.) è la "pubblica fede" in senso oggettivo, intesa come affidamento dei cittadini nei marchi o segni distintivi che individuano le opere dell'ingegno o i prodotti industriali e ne garantiscono la circolazione, e non l'affidamento del singolo, sicché non è necessario per integrare il reato che sia realizzata una situazione tale da indurre il cliente in errore sulla genuinità del prodotto. Al contrario, il reato può sussistere - se la contraffazione sia oggettivamente realizzata - anche se il compratore è stato messo a conoscenza dallo stesso venditore della non autenticità del marchio. Nell'ipotesi di cui all'art. 473 c.p., inoltre, non è neppure necessario per la ricorrenza del reato che il marchio contraffatto raggiunga il consumatore individuale, in quanto la condotta sanzionata consiste nella contraffazione o alterazione, ovvero nell'uso del marchio o del segno distintivo contraffatto o alterato da altri, e detto uso non necessariamente si identifica con la cessione al consumatore potendo realizzarsi in una fase anteriore alla collocazione sul mercato del prodotto recante il marchio contraffatto. Per contraffazione deve intendersi la condotta tesa a far assumere al marchio falsificato qualità tali da ingenerare confusione sull'autentica provenienza del prodotto, con possibile induzione in inganno dei consumatori. L'alterazione, invece, dovrebbe consistere nella modificazione parziale di un marchio genuino. L'oggetto materiale delle condotte sono sempre i marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati e sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà industriale o intellettuale.

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

6. REGOLE GENERALI DI COMPORTAMENTO

Il Personale della Società, a qualsiasi titolo coinvolto nei processi in oggetto, è tenuto a osservare specifiche regole comportamentali, coerentemente con i princìpi deontologici contenuti nel Codice Etico adottato dalla Società.

In particolare, gli Uffici aziendali preposti ed eventuali altri dipendenti direttamente coinvolti nelle operazioni inerenti al processo in oggetto, devono attenersi, nell'ambito dell'erogazione dei servizi e in conformità a quanto stabilito nel Manuale Antiriciclaggio, alle seguenti regole di comportamento:

- identificare la clientela e prevedere la raccolta delle informazioni necessarie alla valutazione del rischio riciclaggio per tutti i rapporti continuativi nonché per i clienti che eseguono operazioni occasionali di importo pari o superiori a € 15.000;
- analizzare le transazioni di importo (singolo o frazionato) pari o superiore a € 15.000, concluse durante tutta la durata del rapporto, al fine di verificare che le stesse siano compatibili con la conoscenza che la Società ha del proprio cliente, delle sue attività commerciali e del suo profilo di rischio, avendo riguardo, se necessario, all'origine dei fondi (controllo costante nel corso del rapporto);
- riscontrare, secondo un approccio basato sul rischio, le informazioni ottenute dalla clientela mediante basi dati autonome, anche esterne alla Società (pubblici registri, *info-provider* esterni);
- verificare periodicamente l'allineamento tra le condizioni di mercato e le condizioni applicate nei rapporti con fornitori, *partner* commerciali e finanziari.

Tutti i dipendenti della Società, nell'esecuzione/erogazione del servizio nei confronti di un cliente soggetto pubblico, devono attenersi alle seguenti regole di comportamento:

- gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle normative vigenti (europee, nazionali, regionali, provinciali e comunali) e con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere, evitando, e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- i rapporti con la Pubblica Amministrazione devono essere improntati alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del ruolo istituzionale, dando puntuale e sollecita esecuzione alle prescrizioni e agli adempimenti richiesti;
- i documenti devono essere elaborati in modo puntuale e in un linguaggio chiaro, oggettivo ed esaustivo;
- tutta la documentazione deve essere verificata e sottoscritta da parte di Personale dotato di idonei poteri, conformemente a quanto previsto dal sistema vigente di procure e deleghe;
- gli Uffici aziendali interessati devono dotarsi di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti nei confronti della Pubblica Amministrazione.

Per prevenire i reati in materia di criminalità organizzata e i reati transnazionali è fatto divieto di:

- trasportare persone o merci che possano, direttamente o indirettamente, integrare ipotesi di traffico illecito o per il cui trasporto siano necessari titoli autorizzativi particolari non connessi al *business* aziendale.

Infine, coerentemente con i princìpi deontologici per prevenire i reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, è fatto divieto di:

- rimettere consapevolmente in circolazione denaro contraffatto, anche ricevuto in buona fede e comunque non conforme alle normative specifiche di settore ed emesse da Banca d'Italia;
- fare un utilizzo improprio degli strumenti di pagamento diversi dal contante;
- alterare, distrarre o mettere a disposizione d'altri gli strumenti di pagamento diversi dal contante;
- alterare i sistemi informatici al fine di modificare o alterare strumenti di pagamento diversi dal contante.

La Società, sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione delle attività aziendali e di prevedere una responsabilità etica dei destinatari, condanna, tramite l'applicazione del Sistema Sanzionatorio previsto nel Codice Etico, i comportamenti difformi ai princìpi sopra riportati.

Qualora la Società si avvalga di società esterne per l'espletamento di attività legate alla gestione ed esecuzione dei Servizi di Vigilanza (cd. corrispondenti) i contratti con tali società devono contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e di impegno al suo rispetto (come già indicato nel Protocollo "Gestione dei rapporti e dei contratti con i clienti enti

pubblici o privati"). Le predette Società dovranno rispettare tutte le modalità operative indicate all'interno del presente protocollo, nonché tutte le regole di condotta presenti nel Codice Etico.

A tal proposito i contratti dovranno essere integrati con la seguente clausola generale, adattata in base allo specifico rapporto contrattuale: "*La Società/corrispondente dichiara di conoscere le prescrizioni contenute nel Codice Etico adottato dalla Società e nel Modello di organizzazione, gestione e controllo ex D.lgs. 231/01, e dichiara di accettarle integralmente, astenendosi da comportamenti a esse contrari. L'eventuale inosservanza di tali princìpi potrà costituire inadempimento contrattuale, legittimando la Società a risolvere il presente contratto ai sensi e per gli effetti dell'articolo 1453 del Codice Civile, fermo restando il diritto al risarcimento dei danni eventualmente subiti dalla Società per effetto di detto inadempimento*."

7. PRESIDI DI CONTROLLO

Le modalità operative che il Personale della Società è tenuto a osservare per i processi sensibili nell'ambito delle attività di Gestione ed esecuzione dei servizi di vigilanza e trasporto ai fini della prevenzione dei reati di cui al D.lgs. 231/2001 sono di seguito descritte. La Società condanna tramite l'applicazione del Sistema Sanzionatorio i comportamenti difformi alle disposizioni seguenti.

7.1 GESTIONE DEI SERVIZI EROGATI

Rangers S.r.l., per mezzo delle dipendenti guardie giurate e con l'uso dei mezzi posti a loro disposizione, eroga i seguenti servizi:

- vigilanza fissa;
- vigilanza saltuaria di zona;
- vigilanza con collegamento di sistemi di allarme e di videosorveglianza;
- intervento su allarme;
- vigilanza fissa antirapina;
- vigilanza fissa mediante l'impiego di unità cinofile;
- servizio di antitaccheggio;
- servizio di trasporto e scorta valori e servizi su apparecchiature automatiche, bancomat e casseforti, per il trasporto valori di denaro contante limitato a euro 100.000,00.
- servizio scorta a beni trasportati con mezzi diversi da quelli destinati al trasporto valori, di proprietà di Rangers S.r.l. o di terzi;
- servizi di vigilanza e di sicurezza complementare e sussidiaria previsti da specifiche norme di legge o di regolamento (D.M. 85/1999, Aeroporti e D.M. 154/2009, Porti ecc.)

Per ciascuno di tali servizi le guardie giurate, devono:

- attenersi esclusivamente alle disposizioni impartite dal Responsabile operativo e dalla Direzione Divisione Vigilanza;
- segnalare tempestivamente eventuali situazioni anomale alla Centrale Operativa, intervenendo in caso di necessità in condizioni di assoluta sicurezza per la propria e l'altrui incolumità;

- compilare, al termine di ogni turno di servizio, un dettagliato rapporto sull'attività svolta solo se vi siano novità, fatti o situazioni degne di rilievo;
- nei servizi ad obiettivi fissi, attendere il cambio prima di lasciare la postazione;
- verificare, prima di intraprendere il servizio, l'efficienza dei mezzi e dell'equipaggiamento in dotazione e segnalare eventuali anomalie riscontrate mediante annotazione sul foglio di marcia e sul rapporto di servizio.

7.1.1 GESTIONE DELL'ATTIVITÀ DI VIGILANZA

La Direzione Divisione Vigilanza cura la formulazione e l'indirizzo della politica aziendale, in relazione agli impegni da assumere e le risorse da destinare allo svolgimento del servizio, tra cui le attività di addestramento e formazione del personale unitamente alla Direzione Risorse Umane Corporate.

Il Responsabile Commerciale, quale interfaccia con il Cliente, cura la gestione dei contatti necessari alla definizione dei requisiti di fornitura e delle specifiche dei servizi richiesti, unitamente al Responsabile dell'area tecnica.

Il responsabile operativo coordina le attività di erogazione del servizio per i vari clienti rispondendone direttamente alla Direzione Vigilanza. Il servizio è predisposto in modo tale da consentire, in caso di necessità - per servizi occasionali o modifiche a quelli ordinari - di essere modificato anche giornalmente; deve essere registrato su apposito software gestionale. Il sevizio è comunicato alle guardie giurate interessate prima dell'inizio dei turni di servizio così come è comunicata ogni variazione intervenuta. Il sevizio riporta i servizi svolti da ciascuna guardia giurata, con l'indicazione dell'orario e della tipologia del servizio stesso.

L'ordine di servizio giornaliero è custodito agli atti dell'Istituto, anche su supporto informatico non modificabile, per almeno due anni e deve essere esibito ad ogni richiesta degli ufficiali ed agenti di pubblica sicurezza, nell'ambito dell'ordinaria attività di controllo.

I Responsabili delle funzioni interessate, le guardie giurate ed il personale dipendente nonché chiunque altro venga a conoscenza degli "ordini di servizio interni" sono tenuti al segreto d'ufficio e ad usare ogni misura o cautela idonea a garantire la riservatezza.

I dipendenti rispettano un regolamento interno, in osservanza di quanto stabilito dagli Organi di Pubblica Sicurezza.

Il monitoraggio del servizio avviene mediante la compilazione, a cura dei componenti delle singole squadre di lavoro, di appositi modelli, controllati dal Responsabile operativo interessato, il quale provvede a monitorare lo stato di avanzamento del servizio.

È predisposto un apposito modulo ("Ordine e rapporto di servizio) contenente i parametri identificativi della prestazione. Il modulo "Rapportino d'intervento" è compilato in caso di accadimenti eccezionali per descrivere l'intervento effettuato e viene firmato dall'operatore coinvolto e dal Responsabile (rappresentante del cliente o rappresentante delle forze dell'ordine

eventualmente intervenute). L'equipaggio ha il compito di segnalare eventuali anomalie nel corso del servizio erogato. La Direzione Divisione Vigilanza ha la responsabilità di riesaminare la modulistica debitamente compilata di ritorno dalle varie sedi lavorative e segnalare eventuali anomalie all'OdV.

Rangers S.r.l. gestisce le chiavi dei siti oggetto di vigilanza in maniera controllata assegnando a ciascuna chiave un codice identificativo che non corrisponde direttamente al nominativo del cliente; inoltre, tale codice identificativo, per motivi di sicurezza, viene variato periodicamente.

Rangers S.r.l. adopera un sistema di informatizzazione che consente di rintracciare e identificare in ogni momento qualsiasi tipologia di servizio erogato, per assicurare e documentare la conformità del servizio ai requisiti richiesti.

Le disposizioni riguardanti le Guardie Particolari Giurate sono contenute nel Protocollo "Selezione, assunzione e gestione del Personale e delle G.P.G.", cui si rinvia.

7.1.2 GESTIONE DELL'ATTIVITÀ DI TRASPORTO

Rangers S.r.l. effettua il servizio di trasporto valori fino a 100.000 euro ed il servizio di scorta a valori trasportati dall'utente nel territorio nazionale ed estero. Nei punti del territorio in cui Rangers S.r.l. non è presente, l'attività viene affidata a dei corrispondenti locali (per la disciplina dei c.d. corrispondenti si rinvia alla *Policy* "Gestione dei corrispondenti").

Rangers S.r.l. adotta un sistema di identificazione del prodotto fornito dal cliente tale da rendere rintracciabile in ogni momento lo stesso, a partire dal momento del ritiro sino al momento della consegna finale. A tal proposito, ogni prodotto viene identificato attraverso una targhetta di identificazione. Il sistema di tracciatura è gestito attraverso una piattaforma informatica che consente di avere uno strumento informativo per il monitoraggio dei valori loro affidati.

Rangers S.r.l., nel trasferimento di somme di denaro o di altri beni e titoli di valore da un luogo ad un altro, equipaggia le dipendenti guardie giurate per l'erogazione del servizio su veicoli di proprietà o nella disponibilità della Società.

In particolare, Rangers S.r.l., cura:

- l'idoneità e la funzionalità dell'equipaggiamento (giubbotti antiproiettile, apparati ricetrasmittenti e di radiolocalizzazione etc.)
- l'adeguatezza dell'armamento;
- l'efficienza dei messi di trasporto prescritti;
- l'efficienza ed efficacia dei sistemi di protezione e di sicurezza;
- le misure di sicurezza e di riservatezza adottate nella definizione dei trasporti e degli itinerari e nella composizione degli equipaggi;
- la qualificazione ed affidabilità del personale impiegato sia nei servizi operativi che in quelli organizzativi;
- l'osservanza del rispetto dei limiti orari e delle alternanze con periodi di riposo previsti per l'impiego delle guardie giurati in tali servizi;

- la registrazione delle operazioni relative ai servizi in apposito registro.

Per i dettagli circa le modalità di erogazione del servizio, si rinvia alle Procedure operative adottate dalla Società e al Manuale della Qualità.

7.2 INSTALLAZIONE DI APPARECCHIATURE DI VIDEOREGISTRAZIONE NELL'AMBITO DEI SERVIZI DI VIGILANZA EROGATI

È compito dell'Area tecnica adottare adeguate misure affinché sia assicurato che le apparecchiature di videosorveglianza installate presso le sedi e i locali dei clienti siano conformi alle specifiche norme contrattuali e in ogni caso il loro utilizzo sia tale da garantire di non incorrere nella commissione dei reati di cui all'art. 24-bis del D.lgs. 231/2001 e in particolare, ai reati di:

- accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies*c.p.).

In particolare, è compito del Responsabile Area Tecnica fare in modo che le apparecchiature installate non siano utilizzate dagli operatori come strumento di divulgazione di immagini o comunicazioni.

Pertanto, il sistema informativo aziendale deve essere in grado di registrare qualsiasi tentativo di copia di immagine o audio realizzato da una specifica postazione.

L'installazione di apparecchiature di videosorveglianza presso le sedi e i locali dei clienti è di norma affidata a fornitori esterni qualificati, inseriti in apposita "lista fornitori".

8. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Conformemente a quanto stabilito nella Parte Generale, fermo restando il suo potere discrezionale di attivarsi con specifici controlli di propria iniziativa o a seguito della segnalazione ricevute, l'OdV effettua periodicamente controlli a campione sulle attività di "Gestione ed esecuzione dei servizi di vigilanza e trasporto", e comunque su ogni attività sensibile individuata nel presente Protocollo, diretti a verificarne l'applicazione in conformità a quanto sopra previsto.

Al fine di verificare il processo in oggetto, i Responsabili delle Funzioni/Uffici interessati e, più in generale, i soggetti muniti di poteri in base al sistema di deleghe e procure sono tenuti ainviare all'Organismo di Vigilanza, con periodicità definita dallo stesso, relazioni inerenti le attività del proprio Ufficio. In particolare, in caso di necessità, le comunicazioni sulle criticità riscontrate devono essere tempestivamente inoltrate da parte dei Responsabili e degli Operatori a conoscenza dei fatti accaduti. Tale attività garantisce il monitoraggio sistematico e formalizzato delle anomalie, eccezioni e deroghe procedurali verificatesi nel periodo di riferimento.

Periodici flussi informativi dovranno pervenire all'Organismo di Vigilanza; ogni anomalia riscontrata nelle procedure operative dovrà essere immediatamente segnalata all'Organismo di Vigilanza.

9. CONSERVAZIONE DELLA DOCUMENTAZIONE

I Responsabili delle Funzioni/Uffici coinvolti nei processi sensibili individuati nel presente protocollo operativo sono responsabili, ciascuno per la parte di propria competenza, della conservazione della documentazione, nel rispetto dei termini di legge, al fine di garantire la tracciabilità delle operazioni aziendali. La documentazione è, inoltre, messa a disposizione, su richiesta, del Consiglio di Amministrazione, del Sindaco Unico e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

GESTIONE DEGLI ADEMPIMENTI PREVISTI IN MATERIA DI SICUREZZA, SALUTE SUL LAVORO E AMBIENTE

INDICE

1. FINALITÀ 2

2.ILSISTEMADEICONTROLLISE 2

2.1. STANDARD DI CONTROLLO GENERALI 2
2.2. STANDARD DI CONTROLLO SPECIFICI 3

3. AMBITO DI APPLICAZIONE 4

4. NORMATIVA DI RIFERIMENTO 4

5. REATI ASTRATTAMENTE PERPETRABILI 5

6. REGOLE DI COMPORTAMENTO IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO 7

6.1 SOGGETTI COINVOLTI E LORO RESPONSABILITÀ 9
6.2 ADEMPIMENTI NORMATIVI 17

7. REGOLE DI COMPORTAMENTO NELLA GESTIONE DEGLI ASPETTI AMBIENTALI 22

7.1.I SOGGETTI COINVOLTI 22
7.2. I PRESIDI DI CONTROLLO 23

8. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 24

9. CONSERVAZIONE DELLA DOCUMENTAZIONE 25

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il Personale deve attenersi nell'ambito del processo di "**Gestione degli adempimenti previsti in materia di sicurezza, salute sul lavoro e ambiente**", al fine di rispettare la normativa antinfortunistica vigente e di garantire l'applicazione dei migliori livelli di sicurezza volti a eliminare e a contenere il rischio di verifica di infortuni all'interno dei locali della Società.

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice Etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società, nelle procedure e istruzioni operative, e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi Sociali, i Dipendenti, i Collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;
- Fornire all'OdV e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei Dipendenti – in via diretta – dei Collaboratori Esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione - di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da - considerati individualmente o collettivamente - integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, nonché delle "*best practice*", prevede con riferimento alle Aree e alle Attività Sensibili individuate:

- *Standard di controllo "generali"*, applicabili a tutte le Attività Sensibili;
- *Standard di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

2.1. STANDARD DI CONTROLLO GENERALI

Gli *standard* di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:

- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;
- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa. Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

2.2. STANDARD DI CONTROLLO SPECIFICI

Sulla base degli *standard* di controllo generali sopra riportati, gli *standard* di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte

effettuate;

- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema delle deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

3. AMBITO DI APPLICAZIONE

Il presente Protocollo si applica a Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 ed è rivolto a tutti i soggetti aziendali coinvolti, a vario titolo, nei processi di gestione degli adempimenti previsti in materia di sicurezza, salute sul lavoro e ambiente.

Le Funzioni/servizi/uffici aziendali coinvolti nelle attività sensibili sono:

- Datore di lavoro;
- Delegato di funzioni;
- Responsabile del Servizio di Prevenzione e Protezione (RSPP);
- Medico competente;
- Responsabile Sistema Gestione Ambientale;
- Responsabile di conformità per la prevenzione della corruzione (RAC);
- RSGSL;
- Safety Assistant;
- Direzione Risorse Umane Corporate;
- Responsabile Health, Safety & Environment (HSE).

Il Datore di Lavoro è il Soggetto che ha la responsabilità della diffusione del presente Protocollo ai propri collaboratori e il compito di garantirne la continua applicazione e aggiornamento.

4. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30*";
- L. 3 agosto 2007 n. 123 "*Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia*";
- D.lgs.9 aprile 2008 n. 81 di attuazione dell'art. 1 della menzionata Legge 123/2007 "*Testo Unico Sicurezza*";
- D.lgs. 3 Agosto 2009 n. 106 "*Disposizioni integrative e correttive del D.lgs. 81/08, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*";
- L. 22 maggio 2015 "*Disposizioni in materia di delitti contro l'ambiente*".

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;
- Codice Etico del Gruppo Battistolli;
- Protocollo "Selezione, Assunzione e gestione del personale";
- Procedure e istruzioni operative;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- DVR e relativi allegati;
- Manuale della Qualità;
- Sistema di Gestione UNI EN ISO 9001:2015; UNI EN ISO 14001:2015; UNI EN ISO 45001:2018, UNI ISO 37001:2016;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

5. REATI ASTRATTAMENTE PERPETRABILI

I reati presupposto (nella forma consumata o tentata) di cui al D.lgs. 231/01 nonché i reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro, introdotti dalla L. 123/2007 (art. 25-*septies*D.lgs.231/01) da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati.

- **Reati colposi commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della sicurezza sul lavoro(art. 25-*septies*):**
  - Omicidio colposo (art. 589 c.p.);

La giurisprudenza maggioritaria accoglie l'interpretazione che ritiene di dover ricollegare, nel caso di reati presupposto colposi, all'interesse o vantaggio dell'ente, non il reato nel suo insieme di condotta ed evento, ma solo la condotta penalmente rilevante. Tale orientamento giurisprudenziale si fonda sulla semplice constatazione che, nel caso di omicidio colposo o lesioni personali colpose in violazione delle norme sulla sicurezza dei lavoratori, l'evento lesivo (ovvero la morte o la lesione) non potrebbe mai rispondere ad un interesse o vantaggio dell'ente, e pertanto l'art. 25-septies non potrebbe mai trovare applicazione. Alla luce di tale interpretazione si comprende chiaramente perchè, nel caso di reati colposi, l'unico criterio che può venire in gioco è quello del vantaggio, rappresentato dai risparmi di spesa derivanti, per esempio, dalla mancata adozione delle necessarie misure antiinfortunistiche. L'interesse, infatti, letto come intenzione dell'agente di favorire l'ente, si scontra inevitabilmente con l'elemento psicologico della colpa.

  - Lesioni personali colpose, gravi o gravissime (art. 590 c.p.).

La Corte di Cassazione, con la sentenza n. 8861/2013, è intervenuta nuovamente sul tema della responsabilità del datore di lavoro per lesioni subite dal dipendente che, durante una trapanazione all'interno di un container, era colpito all'occhio da una scheggia di metallo. Il Supremo Collegio ha condiviso la tesi del giudice di merito secondo cui non sarebbe sussistita la responsabilità del datore di lavoro poiché quest'ultimo «aveva provveduto a fornire, a mezzo dei suoi preposti, i necessari mezzi di protezione (kit contenente, tra gli altri, guanti ed occhiali) ad impartire istruzioni sull'uso degli stessi ed a vigilare sul rispetto delle istruzioni impartite e sull'uso degli occhiali di protezione durante la lavorazione e che, rispetto al puntuale assolvimento di tutti questi obblighi, la condotta del lavoratore aveva assunto il carattere dell'assoluta imprevedibilità». Tale giurisprudenza si trova anche nella sentenza n. 6363/2013, là dove - in conformità con i precedenti giurisprudenziali della Corte di Cassazione - la responsabilità del datore di lavoro non è stata esclusa neppure dalla colpa del lavoratore, poiché la condotta di questi non ha assunto i caratteri dell'"abnormità", risultando eccezionale ed imprevedibile.

Esempio: l'Azienda, nella persona del datore di lavoro, crea prassi illecite che non tengono conto delle norme di sicurezza al fine di velocizzare le tempistiche lavorative e di abbassare i costi relativi all'esercizio delle attività aziendali.

"Il datore di lavoro deve controllare che il preposto, nell'esercizio dei compiti di vigilanza affidatigli, si attenga alle disposizioni di legge e a quelle, eventualmente in aggiunta, impartitegli; ne consegue che, qualora nell'esercizio dell'attività lavorativa si instauri, con il consenso del preposto, una prassi "contra legem", foriera di pericoli per gli addetti, in caso di infortunio del dipendente la condotta del datore di lavoro che sia venuto meno ai doveri di formazione e informazione del lavoratore e che abbia omesso ogni forma di sorveglianza circa la pericolosa prassi operativa instauratasi, integra il reato di lesione colposa aggravato dalla violazione delle norme antinfortunistiche". Cassazione Penale, Sez. 4, Sentenza n. 18638 del 16/01/2004 Ud. (dep. 22/04/2004) Rv. 228344 - 01

Al fine di contrastare la realizzazione della fattispecie di reato, è predisposta una plurisoggettività dei soggetti aziendali coinvolti in materia di sicurezza sul lavoro, realizzando una segregazione delle funzioni e controllo a catena (RSPP, ASPP, Referente per la Sicurezza, RSGSL), nonché apposita procedura per "5.2.4 ATTIVITA' DI FORMAZIONE E INFORMAZIONE" per il personale dipendente.

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25):**

  - Corruzione (artt. 318, 319, 320, 322-*bis* c.p.);

Il reato di corruzione consiste in un accordo fra un pubblico funzionario e un privato, in forza del quale il primo accetta dal secondo un compenso che non gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria). Nella corruzione il pubblico ufficiale ed il privato sono in posizione paritaria, diversamente dalla concussione che invece presuppone lo sfruttamento da parte del funzionario della propria posizione di superiorità alla quale corrisponde una situazione di soggezione nel privato. La fattispecie prevista dall'art. 319 c.p., connotata come quella di cui all'art. 318 c.p. da un rapporto paritetico tra pubblico ufficiale/ incaricato di un pubblico servizio-corrotto e privato-corruttore, se ne differenzia in virtù del fatto che l'atto richiesto al pubblico ufficiale o all'incaricato di un pubblico servizio a fronte della dazione o della promessa di denaro o di altra utilità, risulta contrario ai doveri d'ufficio. In particolare la condotta può concretizzarsi in una omissione o in un ritardo nel compimento di un atto di ufficio ovvero nel compimento di un atto contrario ai doveri di ufficio.

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

Il reato è configurabile solo ove l'offerta del privato o la richiesta del pubblico funzionario non vengano accolte dal destinatario. Tuttavia, ove il rifiuto non sia stato immediato e siano incorse trattative poi non sfociate in un accordo, si ritiene configurabile un tentativo di corruzione del quale rispondono entrambi i soggetti. Nell'istigazione alla corruzione passiva la condotta consiste nell'offrire o nel promettere denaro o altra utilità non dovuti al funzionario. L'offerta o la promessa deve essere seria e concreta ed idonea alla realizzazione dello scopo, tale cioè da indurre il destinatario a compiere o a ritardare un atto dell'ufficio o del servizio ovvero a fare un atto contrario a detti doveri. L'idoneità dell'offerta va valutata con un giudizio "ex ante" che tenga conto dell'entità del compenso, delle qualità personali del destinatario e della sua posizione economica e di ogni altra connotazione del caso concreto.

- **Reati ambientali (art. 25-*undecies*).**

Non esiste una nozione giuridica univoca di ambiente. Merita però di essere menzionata la definizione della sentenza n. 378/2007 Corte Costituzionale, secondo la quale l'ambiente è un bene giuridico che, in senso unitario, coesiste con beni giuridici che hanno ad oggetto componenti del bene "ambiente". L'ambiente, inoltre, è tutelato dall'art. 9 della Costituzione secondo il quale: "La Repubblica …tutela il paesaggio e il patrimonio storico e artistico della Nazione", principalmente al fine di proteggere la salute della persona (art. 32 Cost.). A garanzia della tutela del bene ambiente, sia il codice penale che leggi speciali prevedono precise fattispecie di reato e illeciti amministrativi, cui di recente si sono aggiunte altre specifiche previsioni ed aggravanti grazie alla riforma del 2015.

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex*D.lgs. 231/2001 della Società.

6. REGOLE DI COMPORTAMENTO IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO

Nel particolare ambito dei processi oggetto del Protocollo, oltre ai generali e specifici *standard* di controllo, è necessario attenersi alle ulteriori regole di comportamento come di seguito descritte.

Dettando la disciplina normativa vigente in materia di salute e sicurezza sul lavoro (D.lgs. 81/2008) i princìpi e le regole essenziali per la gestione del rischio in materia di salute e sicurezza, il Modello Organizzativo adottato dalla Società non può prescindere dalla corretta applicazione di detta legislazione e di tutte le altre legislazioni in materia descritte nel paragrafo 4.

I cardini sui cui si regge il sistema di tutele definito dal D.lgs. 81/2008, precisate all'art. 15 del "Testo Unico Sicurezza – misure generali di tutela", possono riassumersi come segue:

- la valutazione di tutti i rischi per la salute e sicurezza;
- la programmazione della prevenzione che tenga in considerazione le condizioni tecniche produttive dell'azienda nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;
- l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;
- la riduzione dei rischi alla fonte;
- la priorità nell'utilizzo di misure di protezione collettiva rispetto a quelle di protezione individuale;
- l'informazione e la formazione adeguate per i lavoratori, i dirigenti e i preposti e i rappresentanti dei lavoratori per la sicurezza;
- le istruzioni per i lavoratori esposti ai rischi;
- la programmazione delle misure ritenute più opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione di codici di condotta e di buone prassi;
- la partecipazione e la consultazione dei lavoratori e dei relativi rappresentanti per la sicurezza;
- la regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità all'indicazione dei produttori.

Il Datore di Lavoro è il Soggetto tenuto a valutare con cura e scrupolosità i rischi per la sicurezza e la salute dei lavoratori e ad adottare misure idonee per evitare o diminuire i rischi in base alle possibilità derivanti dal progresso tecnico, nel rispetto delle prescrizioni contenute nel D.lgs.81/2008.

In particolare, per un'effettiva prevenzione dai rischi, e in conformità anche agli adempimenti prescritti dal D.lgs. 81/2008, è fatta espressa richiesta:

- ai soggetti aziendali (es. il Datore di Lavoro e ai Delegati del Datore di Lavoro) e agli Uffici aziendali coinvolti nella gestione del sistema sicurezza di svolgere i compiti loro attribuiti dalla Società nel rispetto delle deleghe e delle procure conferite, nonché delle procedure aziendali esistenti, avendo cura di informare e formare il personale che, nello svolgimento delle proprie attività, sia esposto a rischi connessi alla sicurezza;
- ai soggetti nominati dalla Società ai sensi del D.lgs. 81/2008 (es. i Responsabili del Servizio di Prevenzione e Protezione (RSPP), gli Addetti al Servizio di Prevenzione e Protezione (ASPP), gli Incaricati dell'attuazione delle misure di prevenzione incendi, lotta antincendio, evacuazione dei lavoratori in caso di pericolo, gli Addetti al Primo Soccorso) di svolgere, ciascuno nell'ambito delle proprie competenze e attribuzioni, i compiti di sicurezza specificamente affidati dalla normativa vigente e previsti nel "*sistema sicurezza*" della Società;
- ai preposti di vigilare sulla corretta osservanza, da parte di tutti i lavoratori degli stabilimenti, delle misure e delle procedure di sicurezza adottate dalla Società, segnalandone eventuali carenze o disallineamenti del sistema sicurezza, nonché comportamenti a esso contrari;
- a tutti i dipendenti di aver cura, secondo quanto indicato dal disposto legislativo e nel sistema di sicurezza aziendale, della propria sicurezza e salute e di quella delle altre persone presenti sul luogo di lavoro, osservando le misure, le procedure di sicurezza e le istruzioni operative fornite dalla Società, e facendo utilizzo, laddove sia obbligatorio, dei Dispositivi di Protezione Individuale (DPI) consegnati dalla stessa. È, inoltre, dovere dei lavoratori sottoporsi ai controlli sanitari, partecipare ai corsi di formazione e segnalare al preposto, o al RSPP ovvero, al medesimo Datore di Lavoro eventuali carenze delle attrezzature impiegate e di tutte le condizioni di pericolo che vengono di volta in volta riscontrate.

Gli adempimenti nei confronti degli Enti Pubblici, preposti al controllo dell'applicazione della normativa in materia antinfortunistica, e la predisposizione della relativa documentazione devono essere effettuati attenendosi ai seguenti principi:

- tempestività;
- massima diligenza e professionalità;
- indicazione di informazioni complete, accurate, fedeli e veritiere;
- preventiva verifica e sottoscrizione, da parte del Delegato in materia di sicurezza ai sensi dell'art. 16 del D.lgs. 81/2008, di tutte le informazioni fornite a tali Enti.

I rapporti con i funzionari degli Enti Pubblici preposti al controllo dell'applicazione della normativa in materia antinfortunistica devono essere gestiti dal Delegato in materia di sicurezza ai sensi dell'art. 16 del D.lgs. 81/2008, vale a dire, dai soggetti aziendali autorizzati dal Delegato in materia di sicurezza. Laddove possibile detti rapporti dovranno essere gestiti preferibilmente da almeno due soggetti aziendali.

Qualora la Società si avvalga dell'assistenza di consulenti/professionisti/società esterne per la predisposizione del sevizio e della documentazione rilevante in materia di sicurezza ovvero

nell'esecuzione di specifiche attività, i contratti con tali soggetti devono contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e, in particolare, delle norme comportamentali sancite nel Codice Etico della Società, e di impegno al loro rispetto. A tale proposito i contratti dovranno essere integrati con le seguenti clausole generali, adattate in base allo specifico rapporto contrattuale: "*Il consulente/professionista dichiara di conoscere le prescrizioni contenute nel Codice Etico adottato da Rangers S.r.l., e dichiara, inoltre, di accettarle integralmente, astenendosi da comportamenti ad esse contrari. Il consulente/professionista, nel caso in cui sia dipendente o collabori con Enti Pubblici, dichiara di aver assolto tutti gli adempimenti da questi eventualmente richiesti e/o previsti dalle leggi in vigore per l'assunzione di altri incarichi professionali. L'eventuale inosservanza di tali principi potrà costituire inadempimento contrattuale, legittimando la Società a risolvere il presente contratto ai sensi e per gli effetti dell'articolo 1453 del Codice Civile, fermo restando il diritto al risarcimento dei danni eventualmente subiti dalla Società per effetto di detto inadempimento.*"

La Società condanna, tramite l'applicazione del Sistema Sanzionatorio, i comportamenti difformi ai principi e alle regole comportamentali sopra riportate.

6.1 SOGGETTI COINVOLTI E LORO RESPONSABILITÀ

La normativa antinfortunistica istituisce una serie di figure cui assegna peculiari prerogative e responsabilità nel sistema di tutela della sicurezza, al fine di concorrere, anche attraverso una specifica competenza tecnica, al miglior perseguimento della sicurezza aziendale.

Si riporta di seguito l'elenco dei soggetti coinvolti, nell'ambito del D.lgs. 81/2008, per l'identificazione di ruolo e responsabilità.

DATORE DI LAVORO

Sulla base di quanto richiamato dal disposto legislativo, il Datore di Lavoro in relazione alla natura dell'azienda, valuta i rischi per la sicurezza e per la salute dei lavoratori. In particolare, ai sensi dell'art. 17 del D.lgs. 81/2008, il Datore di Lavoro è responsabile direttamente di:

- valutare tutti i rischi per la sicurezza e per la salute dei lavoratori con la conseguente elaborazione del documento di cui all'art. 28 del Decreto (DVR);
- designare il Responsabile del Servizio di Prevenzione e Protezione dei rischi.

Inoltre, ai sensi dell'art. 18 del D.lgs. 81/08, il Datore di lavoro e/o il Delegato del Datore di lavoro è responsabile di:

- nominare il Medico competente;
- designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei lavoratori in caso di pericolo grave e immediato, di pronto soccorso e, comunque, di gestione dell'emergenza;
- individuare il preposto o i preposti per l'effettuazione delle attività di vigilanza di cui all'articolo 19;
- tenere conto, nell'affidare i compiti ai lavoratori, delle capacità e delle condizioni degli stessi in rapporto alla loro salute e sicurezza;

- fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentiti i RSPP e il medico competente;
- prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevute adeguate istruzioni e specifico addestramento accedano alle zone che li espongono a un rischio grave e specifico;
- richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;
- inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richiedere al medico competente l'osservanza degli obblighi previsti a suo carico dal D.lgs. 81/08;
- comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro;
- adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37;
- astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
- consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;
- consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento afferente alla valutazione dei rischi nonché consentire al medesimo rappresentante di accedere ai dati relativi agli infortuni sul lavoro di cui alla lettera r) dell'art.18 del D.lgs.81/08;
- prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;
- comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del certificato medico, a fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni; l'obbligo di comunicazione degli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni si considera comunque assolto per mezzo della denuncia di cui all'articolo 53 del testo unico delle disposizioni per l'assicurazione

obbligatoria contro gli infortuni sul lavoro e le malattie professionali, di cui al decreto del Presidente della Repubblica 30 giugno 1965, n. 1124;

- consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50 del D.lgs. 81/08;
- adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43 del D.lgs. 81/08. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;
- nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro;
- convocare la riunione periodica di cui all'articolo 35;
- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza; in fase di prima applicazione l'obbligo di cui alla presente lettera riguarda i nominativi dei rappresentanti dei lavoratori già eletti o designati;
- vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità;
- verificare, in caso di affidamento dei lavori interni all'azienda a ditte appaltatrici, l'idoneità tecnico-professionale delle ditte e dei lavoratori autonomi e approvare i lavori da affidare in appalto o contratto d'opera ai sensi della normativa in vigore, nonché mettere in atto le comunicazioni/azioni previste dal disposto legislativo quali l'elaborazione del "Documento Unico di Valutazione dei Rischi da Interferenze" (DUVRI);
- formare i responsabili dei posti di lavoro fissi dell'impresa per quanto concerne l'effettuazione dei monitoraggi di primo livello e verificare che tali monitoraggi siano effettuati (per questa specifica funzione il Datore di lavoro delega la Direzione delle Risorse Umane).

Inoltre, ai sensi dell'art. 18 comma 2, il Datore di Lavoro fornisce al Servizio di Prevenzione e Protezione (SPP) e al Medico competente informazioni in merito a:

- la natura dei rischi;
- l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
- la descrizione degli impianti e dei processi produttivi;
- i dati relativi agli infortuni sul lavoro e alle malattie professionali;
- i provvedimenti adottati dagli organi di vigilanza.

RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE (RSPP)

Il Servizio di Prevenzione e Protezione è utilizzato dal Datore di lavoro. Il Responsabile del Servizio di Prevenzione e Protezione (ai sensi dell'art. 33 comma 1 del D.lgs. 81/2008) è responsabile di:

- collaborare con il Datore di Lavoro all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro;
- elaborare le misure preventive e protettive e i sistemi di controllo di tali misure;
- elaborare le procedure di sicurezza per le varie attività aziendali;
- proporre programmi di informazione e formazione dei lavoratori;
- partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35;
- favorire l'attuazione presso i posti di lavoro fissi dell'impresa (sede, magazzini, officine, etc.) delle vigenti norme di prevenzione verificando che sia redatto il documento di valutazione dei rischi con riferimento alle attività fisse dell'impresa;
- fornire ai lavoratori le informazioni di cui all'art. 36 del Decreto (es. sui rischi per la salute e sicurezza sul lavoro; sulle procedure di primo soccorso, antincendio; sui nominativi del RSPP, ASPP, Medico competente ecc).

MEDICO COMPETENTE

Il Medico Competente, ai sensi dell'art. 25 del D.lgs. 81/2008, ha le seguenti responsabilità:

- collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, all'attività di formazione e informazione nei confronti dei lavoratori, per la parte di competenza, e all'organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la sorveglianza sanitaria (art. 41), attraverso protocolli sanitari definiti in funzione dei rischi specifici, esprimendo giudizi di idoneità alla mansione specifica al lavoro;
- istituire, aggiornare e custodire, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria;
- consegnare al Datore di lavoro, alla cessazione dell'incarico, la documentazione sanitaria in suo possesso;
- consegnare al lavoratore, alla cessazione del rapporto di lavoro, copia della cartella sanitaria e di rischio;
- fornire informazioni ai lavoratori sul significato della sorveglianza sanitaria cui sono sottoposti nonché sui risultati della stessa;

- comunicare per iscritto, in occasione delle riunioni periodiche (art. 35) al datore di lavoro, al RSPP, ai RLS i risultati anonimi collettivi della sorveglianza sanitaria effettuata e fornisce indicazioni sul significato di detti risultati ai fini della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori;
- visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa che stabilisce in base alla valutazione dei rischi; l'indicazione di una periodicità diversa dall'annuale deve essere comunicata al Datore di Lavoro ai fini della sua annotazione nel documento di valutazione dei rischi;
- partecipa alla programmazione del controllo dell'esposizione dei lavoratori i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della sorveglianza sanitaria;
- informare per iscritto il Datore di Lavoro e il lavoratore qualora, a seguito degli accertamenti sanitari, esprima un giudizio sull'inidoneità parziale o temporanea o totale del lavoratore.

Il Medico competente è tenuto a comunicare, mediante autocertificazione, il possesso dei titoli e requisiti di cui all'articolo 38 del D.lgs. 81/2008 al Ministero della salute entro il termine di sei mesi dall'entrata in vigore del decreto stesso.

RAPPRESENTANTE DEI LAVORATORI PER LA SICUREZZA (RLS)

Il Rappresentante dei Lavoratori per la Sicurezza (art. 50), fatto salvo quanto stabilito in sede di contrattazione collettiva, ha le seguenti attribuzioni:

- accede ai luoghi di lavoro in cui si svolgono le lavorazioni;
- è consultato preventivamente e tempestivamente in ordine alla valutazione dei rischi, alla individuazione, programmazione, realizzazione e verifica della prevenzione nell'azienda o unità produttiva;
- è consultato sulla designazione del responsabile e degli addetti al servizio di prevenzione, alla attività di prevenzione incendi, al primo soccorso, alla evacuazione dei luoghi di lavoro e del medico competente;
- è consultato in merito all'organizzazione della formazione di cui all'articolo 37;
- riceve le informazioni e la documentazione aziendale inerente alla valutazione dei rischi e le misure di prevenzione relative, nonché quelle inerenti alle sostanze e alle miscele pericolose, alle macchine, agli impianti, alla organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali;
- riceve le informazioni provenienti dai servizi di vigilanza;
- riceve una formazione adeguata e, comunque, non inferiore a quella prevista dall'art. 37;
- promuove l'elaborazione, l'individuazione e l'attuazione delle misure di prevenzione idonee a tutelare la salute e l'integrità fisica dei lavoratori;
- formula osservazioni in occasione di visite e verifiche effettuate dalle autorità competenti, dalle quali è, di norma, sentito;

- partecipa alla riunione periodica di cui all'art. 35;
- fa proposte in merito alla attività di prevenzione;
- avverte il responsabile della azienda dei rischi individuati nel corso della sua attività;
- può fare ricorso alle autorità competenti qualora ritenga che le misure di prevenzione e protezione dai rischi adottate dal Datore di Lavoro dai dirigenti e i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.

HSE MANAGER

L'HSE garantisce, con il supporto dei consulenti esterni in materia di sicurezza, l'attuazione delle politiche in materia di salute, sicurezza sul lavoro e ambiente all'interno delle Società del Gruppo. In particolare, l'HSE Manager si occupa di:

1. Analizzare il Sistema attualmente in uso e delineare un percorso di implementazione e sviluppo del Sistema di Gestione Sicurezza e Ambiente (SGAS) del Gruppo e Responsabilità Sociale (RS) in conformità alla normativa di riferimento e con le politiche aziendali;
2. Rivedere le procedure in uso nell'ottica di dare loro una maggiore efficacia o, se necessario, sostituirle con nuove procedure;
3. Pianificare, organizzare e gestire azioni per il miglioramento continuo del Sistema SGAS ed RS: studio della fattibilità dei progetti, controllo dei costi, predisposizione e rispetto del budget coordinando l'attività delle risorse coinvolte nei progetti;
4. Supportare le Direzioni del Gruppo nell'individuazione delle prescrizioni legislative e requisiti normativi generali applicabili e promuoverne il recepimento attraverso l'adeguamento del Sistema di Gestione;
5. Contribuire all'individuazione dei fattori di rischio e alla valutazione dei rischi nel rispetto della normativa vigente;
6. Garantire che il personale coinvolto nelle attività di gestione dei Sistemi sia adeguatamente formato e aggiornato;
7. Collaborare con le funzioni aziendali interessate all'individuazione e alla validazione delle metodologie e delle tecniche per il controllo dei processi e supportarle nella prevenzione e correzione delle situazioni di non conformità emerse;
8. Partecipare alle riunioni con i rappresentanti dei lavoratori per la sicurezza, con il medico competente, col datore di lavoro. Organizzare i piani di intervento e le misure correttive individuate durante le riunioni.
9. Svolgere azioni di monitoraggio del sistema SGAS ed RS, attraverso verifiche ispettive interne sui processi e sulle aree funzionali, per sincerarsi che tutte le attività dell'organizzazione si svolgano nel rispetto delle procedure definite dall'azienda;
10. Effettuare l'analisi di problematiche e non conformità, individuando soluzioni organizzative e tecnologiche eco-compatibili e funzionali agli adeguamenti prescritti e definire le azioni correttive;

11. Monitorare sia la predisposizione della documentazione prevista dal Sistema SGAS ed RS (manuali, procedure e relazioni tecniche) che la revisione e l'aggiornamento periodico;
12. Relazionarsi con gli enti di controllo esterni e interni all'azienda avendo la responsabilità di tutto l'iter burocratico richiesto dagli organismi di vigilanza e controllo dei sistemi RS e SGAS per il conseguimento e le verifiche periodiche delle certificazioni;
13. Garantire, mediante il coordinamento di team dedicati, circa l'ottenimento ed il mantenimento di certificazioni in area RS e SGAS;
14. Tenere o verificare la tenuta della documentazione normativa favorendone la diffusione all'interno dell'azienda;
15. Tenere o verificare che sia tenuta la documentazione relativa agli infortuni sul lavoro e alle anomalie riscontrate (ivi compresi i verbali di ispezione delle autorità preposte ai controlli) individuando le cause di infortuni e anomalie e proporre le misure necessarie per evitarli nel futuro;
16. Definire o verificare che sia definito il programma di formazione dei dipendenti controllandone almeno la rispondenza a quanto previsto dalle leggi vigenti;
17. Definire o verificare che siano definite le procedure tecniche di uso, manutenzione e monitoraggio di macchine, impianti, attrezzature e DPI;
18. Verificare che siano definiti i piani di sicurezza "preliminari".

RESPONSABILI DI FUNZIONE (DIRIGENTI E PREPOSTI)

I Responsabili di Funzione, nelle rispettive aree di competenza:

- identificano le attività, processi o servizi che possono comportare rischi per la salute e sicurezza nei luoghi di lavoro;
- collaborano nella definizione dei fattori di rischio e nella valutazione dei rischi.

In particolare, i preposti individuati dal Datore di Lavoro, ai sensi dell'art. 19 del D.lgs. 81/08, secondo le loro attribuzioni e competenze, devono:

- sovrintendere e vigilare sull'osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di rilevazione di comportamenti non conformi alle disposizioni e istruzioni impartite dal Datore di lavoro e dai dirigenti ai fini della protezione collettiva e individuale, intervenire per modificare il comportamento non conforme fornendo le necessarie indicazioni di sicurezza. In caso di mancata attuazione delle disposizioni impartite o di persistenza dell'inosservanza, interrompere l'attività del lavoratore e informare i superiori diretti;

- verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;
- segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
- in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza, se necessario, interrompere temporaneamente l'attività e, comunque, segnalare tempestivamente al datore di lavoro e al dirigente le non conformità rilevate;
- frequentare appositi corsi di formazione secondo quanto previsto dall'art. 37.

R-SGSL

Le Linee guida UNI-INAIL (2001) definiscono R-SGSL il "*soggetto incaricato dal datore di lavoro, dotato di adeguata capacità ed autorità all'interno dell'azienda, a cui è affidato in tutto o in parte il compito, indipendentemente da ulteriori responsabilità aziendali, di coordinare e verificare che il SGSL sia realizzato in conformità alle linee guida UNI-INAIL*".

R-SGSL collabora strettamente con RSPP ed esamina i vari argomenti in un'ottica più orientata al sistema rispetto a quella del RSPP.

Il responsabile R-SGSL si impegna a prestare tutte le attività previste dalle normative vigenti e, in particolare, si occupa di:

- tenere la documentazione relativa alla gestione del SGSL;
- proporre al datore di lavoro le misure per favorire il miglioramento del SGSL;
- verificare presso i fornitori e i subappaltatori la presenza di SGSL o di loro elementi prevedendo, in mancanza di tali elementi, l'intensificazione delle riunioni di coordinamento;
- riferire periodicamente all'Organismo di vigilanza sul funzionamento del SGSL, in particolare riguardo gli esiti del monitoraggio redigendo, almeno una volta l'anno, un'apposita relazione.

6.2 ADEMPIMENTI NORMATIVI

Le principali attività connesse con gli adempimenti in materia di sicurezza e prevenzione sono individuabili nelle seguenti:

- valutazione dei rischi concretamente presenti e redazione della relazione sulla valutazione;
- definizione dell'"Organigramma Aziendale della Sicurezza" attraverso una precisa individuazione dei seguenti soggetti:
  - Datore di Lavoro;
  - Delegato in materia di sicurezza ai sensi dell'art. 16 del D.lgs. 81/2008;
  - Dirigenti e Preposti;
  - Medico competente;
  - Responsabili del Servizio di Prevenzione e Protezione (RSPP);
  - Rappresentante dei lavoratori per la sicurezza (RLS);
- designazione dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione in caso di pericolo, di salvataggio, di pronto soccorso, e di gestione delle emergenze quale designazione preventiva, tenendo conto delle dimensioni dell'azienda e dei rischi presenti;
- riunione annuale del Servizio di Prevenzione e Protezione;
- attività di Formazione e Informazione di tutti i lavoratori e, in particolare dei lavoratori più esposti ai rischi;
- comunicazioni agli Enti Pubblici competenti;
- aggiornamento delle misure di prevenzione e protezione in relazione ai mutamenti organizzativi che assumano rilevanza ai fini della salute e della sicurezza sul lavoro, ovvero di utilizzo di nuovi impianti o attrezzature nell'ambito del ciclo produttivo, in relazione al grado di evoluzione dei mezzi tecnici utilizzati per la prevenzione e protezione, e sulla base della conseguente rivalutazione del rischio nel Documento di Valutazione dei Rischi (DVR) relativo alla Filiale.

6.2.1. VALUTAZIONE DEI RISCHI E DOCUMENTO DI VALUTAZIONE DEI RISCHI

L'art. 28 del D.lgs. 81/2008 definisce in termini più precisi l'oggetto della valutazione dei rischi e il contenuto del DVR, di cui richiede data certa.

Sulla base di quanto disposto, il Datore di Lavoro è obbligato a effettuare la valutazione dei rischi per la sicurezza e per la salute dei lavoratori e a elaborare/redigere un documento di valutazione (DRV – Documento di Valutazione dei Rischi) contenente, principalmente, le seguenti informazioni:

- una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
- misure di prevenzione e protezione conseguenti agli esiti della valutazione;

- il programma delle misure ritenute opportune per garantire, nel tempo, il miglioramento dei livelli di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del responsabile del Servizio di Prevenzione e Protezione dai rischi, del Rappresentante dei Lavoratori per la sicurezza e del Medico Competente che ha partecipato alla valutazione dei rischi;
- l'individuazione delle mansioni che eventualmente espongano i lavoratori a rischi specifici che richiedono una particolare capacità professionale, esperienza e formazione;
- l'individuazione di tutti i rischi, ivi inclusi quelli collegati allo stress lavoro-correlato, alle lavoratrici in stato di gravidanza e alle differenze di genere, età e provenienza delle persone.

Il DVR è soggetto a una costante verifica del permanere della sua validità ed efficacia nel tempo, con obbligo di aggiornamento ogni qualvolta mutino le situazioni di rischio ivi descritte o si aggiungano nuovi ambienti di lavoro o nuovi macchinari/impianti.

Il Datore di Lavoro elabora tale documento, tenendo conto della normativa vigente, in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione e con il Medico Competente, previa consultazione del Rappresentante dei Lavoratori per la Sicurezza.

Ogni quattro anni la Società deve inoltre provvedere alla valutazione del rischio rumore effettuata ai sensi del D.lgs. 195/2006.

La suddetta documentazione, firmata dal Datore di Lavoro, deve essere conservata accuratamente dallo stesso presso la sede della Società ovvero presso ciascuna Filiale, rendendola disponibile per la consultazione ai soggetti coinvolti nell'ambito delle tematiche concernenti la salute e sicurezza sul lavoro aziendale, agli organi societari nonché agli Enti esterni preposti al controllo.

6.2.2. DEFINIZIONE DELL'"ORGANIGRAMMA AZIENDALE DELLA SICUREZZA"

La Società è responsabile di una chiara e precisa individuazione dei ruoli e delle attribuzioni in materia di salute e sicurezza sul lavoro attraverso la previsione di un "Organigramma aziendale della sicurezza", nel quale devono essere indicati in modo puntuale:

- Datore di Lavoro ;
- Delegato in materia di sicurezza ai sensi dell'art. 16 del D.lgs. 81/2008;
- Eventuali Dirigenti e Preposti;
- Medico competente;
- Responsabili del Servizio di Prevenzione e Protezione (RSPP);
- HSE Manager;

- Rappresentante dei Lavoratori per la Sicurezza (RLS);

Tutti i soggetti indicati nell'Organigramma aziendale della sicurezza devono essere stati formalmente identificati con formale nomina e/o delega. Tale documento è incluso nel Documento di Valutazione dei Rischi della Società e pubblicato nella "bacheca" aziendale.

6.2.3. RIUNIONE ANNUALE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE

Sulla base di quanto disposto dall'art. 35, nelle aziende e nelle unità produttive che occupano più di 15 lavoratori, il Datore di Lavoro, direttamente o tramite il Servizio di Prevenzione e Protezione, indìce, almeno una volta l'anno o in occasione di significative variazioni delle condizioni di esposizione al rischio, una riunione cui partecipano:

- il Datore di Lavoro o un suo rappresentante;
- il Responsabile del Servizio di Prevenzione e Protezione da rischi (se diverso dal Datore di Lavoro);
- il Medico competente;
- il/i Rappresentante/i dei Lavoratori per la Sicurezza.

Nel corso della riunione, il Datore di Lavoro sottopone ai partecipanti il Documento di Valutazione dei Rischi, l'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria, i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale e i programmi di informazione e formazione dei dirigenti, dei preposti e dei lavoratori ai fini della sicurezza e della protezione della loro salute.

Della riunione deve essere redatto un verbale che è a disposizione dei partecipanti per la consultazione.

6.2.4. ATTIVITÀ DI FORMAZIONE E INFORMAZIONE

In relazione a quanto disposto dall'art.36 e dall'art. 37 del D.lgs. 81/2008 il Datore di Lavoro provvede affinché ciascun lavoratore riceva una adeguata informazione e si assicura che ciascun lavoratore consegua una formazione appropriata in materia di salute e sicurezza, anche rispetto alle conoscenze linguistiche, con particolare riferimento a:

- concetti di rischio, danno, prevenzione, protezione, organizzazione della prevenzione aziendale, diritti e doveri dei vari soggetti aziendali, organi di vigilanza, controllo, assistenza;
- rischi riferiti alle mansioni e ai possibili danni e alle conseguenti misure e procedure di prevenzione e protezione caratteristiche del settore o comparto di appartenenza dell'azienda.

Inoltre, con la conversione in legge del D.L. n. 146/2021, è stata introdotta un'ulteriore attività di formazione specifica per il datore di lavoro, i dirigenti e i preposti da svolgersi ogni qualvolta sia reso necessario in ragione dell'insorgenza di nuovi rischi o dell'evoluzione degli stessi. In

particolare, la durata, i contenuti minimi e la modalità di formazione sono stabiliti con Accordo mediante Conferenza permanente tra Stato e Regioni, volto a garantire:

a) l'individuazione della durata, dei contenuti minimi e delle modalità della formazione obbligatoria a carico del datore di lavoro;

b) l'individuazione delle modalità della verifica finale di apprendimento obbligatoria per i discenti di tutti i percorsi formativi e di aggiornamento obbligatori in materia di salute e sicurezza sul lavoro e delle modalità delle verifiche di efficacia della formazione durante lo svolgimento della prestazione lavorativa.

Le attività di formazione e informazione sono gestite dal Responsabile del Servizio di Prevenzione e Protezione d'intesa con il Responsabile HSE e la Direzione Risorse Umane Corporate. Il RSPP provvede a:

- redigere un piano programmatico di formazione (con indicazione dei soggetti che ne usufruiranno e degli argomenti del corso);
- dare evidenza del programma di formazione effettuato. Ogni partecipante deve firmare il registro presenze che sarà poi conservato come allegato al materiale formativo;
- consegnare a ogni neo-assunto un manuale che sintetizzi i principali obblighi e i principali adempimenti in materia di sicurezza e salute sul lavoro, nonché i rischi ivi presenti e le misure di prevenzione e protezione adottate.

La documentazione di cui sopra è archiviata presso l'ufficio del Responsabile del Servizio di Prevenzione e Protezione. La formazione dei lavoratori e dei loro rappresentanti deve essere periodicamente ripetuta in relazione all'evoluzione dei rischi o all'insorgenza di nuovi fattori di rischio.

6.2.5. FLUSSO INFORMATIVO AL DATORE DI LAVORO

Il Datore di lavoro della Società, ai sensi dell'art. 16 del D.lgs. 81/08, ha delegato le funzioni in materia di salute e sicurezza sui luoghi di lavoro – a esclusione degli obblighi espressamente non delegabili ex art. 17 – a un Soggetto in possesso dei requisiti idonei per l'espletamento dei compiti e delle funzioni allo stesso attribuiti. In particolare,

Al fine di garantire l'attività di alta vigilanza in capo al Datore di lavoro, il Delegato, a cadenza semestrale, inoltra al Datore di lavoro uno specifico report relativo all'attività espletata. In particolare, evidenziando:

- lo status dell'attività di informazione/formazione/addestramento, con l'indicazione delle eventuali scoperture e delle azioni di rimedio proposte;
- lo status della sorveglianza sanitaria, con indicazione del numero di visite mediche preventive/periodiche, con l'indicazione delle eventuali scoperture e delle azioni di rimedio proposte;
- il numero e la tipologia di infortuni eventualmente verificatisi, con indicazione delle azioni poste in essere;

- l'attività di verifica espletata in relazione alla rispondenza dei macchinari, degli strumenti e degli apparati aziendali alla disciplina antinfortunistica di prevenzione, di protezione, di sicurezza e di igiene del lavoro;
- l'attività di verifica espletata in relazione all'adeguatezza dei presidi e delle procedure aziendali adottate in materia di salute e sicurezza sui luoghi di lavoro, con l'indicazione delle eventuali azioni di miglioria;
- l'attività di verifica espletata in materia di corretta fornitura dei dispositivi di protezione individuale ai lavoratori;
- le evidenze emerse dalla riunione periodica ex art. 35 nonché dell'attività di controllo espletata dagli ulteriori Soggetti coinvolti.

Ciò al solo fine di consentire l'espletamento, da parte del Datore di lavoro, dell'attività di vigilanza ex art. 16 comma 3 del D.lgs. 81/08 inerente al corretto svolgimento delle proprie funzioni da parte del soggetto delegato, attuato anche mediante i flussi informativi dei Soggetti coinvolti nella verifica della corretta attuazione del modello di gestione della sicurezza ex. art. 30 comma 4.

È d'uopo segnalare a tal proposito che, ai sensi dell'art. 30 del D.lgs. 81/08, l'attuazione di un corretto modello di gestione della sicurezza sul lavoro esonera il Datore di lavoro dalla responsabilità amministrativa di cui al D.lgs. 231/01. Tuttavia, affinché tale modello abbia l'effettiva efficacia esimente è necessario che lo stesso sia:

1. adottato ed efficacemente attuato in azienda per l'adempimento degli obblighi relativi:
    - al rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
    - alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
    - alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazione dei rappresentanti dei lavoratori per la sicurezza;
    - alle attività di sorveglianza sanitaria;
    - alle attività di informazione e formazione dei lavoratori;
    - alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
    - all'acquisizione di documentazioni e certificazioni obbligatorie di legge;
    - alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.
2. deve prevedere idonei sistemi di registrazione degli eventi;
3. deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;

4. deve prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo sono necessari quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Inoltre, ai sensi dell'art. 16 comma 4, l'obbligo di vigilanza in capo al Datore di lavoro si intende assolto in caso di adozione ed efficace attuale del modello di verifica e controllo di cui all'articolo 30 comma 4. Resta ferma, invece, la responsabilità e la vigilanza del Delegato, come previsto dall'art. 16 e dalla consolidata giurisprudenza in materia, relativamente alla concreta, minuta conformazione delle singole lavorazioni.

6.2.6. REVISIONE DOCUMENTAZIONE E ADEMPIMENTI PERIODICI DELLE MISURE DI PREVENZIONE

Di seguito si riportano i principali adempimenti periodici e/o di revisione della documentazione:

- il Datore di Lavoro rielabora la valutazione e il Documento di Valutazione dei Rischi, in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei lavoratori;
- il Datore di Lavoro/il Delegato in materia di sicurezza ai sensi dell'art. 16 del D.lgs.81/2008 ha il compito di curare che il Responsabile del Servizio di Prevenzione e Protezione dai rischi aggiorni le misure di prevenzione incendi e lotta antincendio, di evacuazione in caso di pericolo grave, di salvataggio, di pronto soccorso, in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza del lavoro, ovvero in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- il Responsabile del Servizio di Prevenzione e Protezione dai rischi nonché i relativi addetti sono obbligati, su iniziativa aziendale, a frequentare specifici corsi di aggiornamento con cadenza almeno triennale.

7. REGOLE DI COMPORTAMENTO NELLA GESTIONE DEGLI ASPETTI AMBIENTALI

7.1.I SOGGETTI COINVOLTI

7.1.1. LA SEGREGAZIONE DEI RUOLI E DELLE RESPONSABILITÀ

Le responsabilità connesse alla gestione degli aspetti ambientali sono così suddivise:

- **Responsabile Sistema Gestione Ambientale (RGA)**,alle dirette dipendenze del CdA, assume la piena e totale responsabilità dell'applicazione, dell'implementazione e manutenzione del Sistema di Gestione di Ambientale e di tutte le attività correlate a esso. È coadiuvato dagli altri responsabili di processo, nella programmazione e corretto svolgimento delle attività di controllo, analisi e miglioramento del sistema.
- **Gruppo di Lavoro**, formato da personale interno e da consulenti esterni con conoscenze specifiche della materia e dei rischi connessi alle problematiche ambientali.

- **La Direzione** collabora con il RGA nell'identificazione degli aspetti ambientali e nella valutazione della significatività degli aspetti ambientali; approva il Registro e i relativi aggiornamenti; approvale variazioni da apportare al Sistema di Gestione Ambientale.

7.1.2. LA TRACCIABILITÀ

L'identificazione degli aspetti ambientali avviene mediante l'utilizzo di strumenti che hanno l'obiettivo di raccogliere i dati e le informazioni necessarie. Più precisamente, la Direzione costituisce un Gruppo di lavoro, al fine di realizzare l'identificazione e la valutazione degli impatti ambientali significativi relativi alle attività produttive dell'organizzazione. Le modalità dell'analisi sono contenute nella PO SGA01 "Conduzione dell'analisi ambientale iniziale", cui si rinvia.

Per ogni aspetto ambientale considerato (scarichi dei corpi idrici, emissioni in atmosfera, utilizzo di risorse naturali, rifiuti, rumori, impatto visivo, contaminazione del suolo), viene valutato l'impatto sull'ambiente. Se l'impatto è negativo, cioè non trascurabile, allora l'aspetto ambientale è considerato significativo.

Il Gruppo di Lavoro ha la responsabilità della conduzione delle fasi di identificazione degli aspetti e di valutazione degli impatti ambientali correlati alle attività/prodotti dell'organizzazione.

Il RGA è responsabile dell'individuazione di variazioni nelle attività o prodotti tali da indurre variazioni degli aspetti e degli impatti ambientali significativi.

Tutta la documentazione raccolta per la corretta effettuazione dell'analisi ambientale iniziale è presentata alla Direzione per il Riesame del Sistema di Gestione Ambientale.

7.2. I PRESIDI DI CONTROLLO

Le procedure operative descrivono la struttura organizzativa, le responsabilità e le modalità adottate dall'azienda per la gestione ambientale e costituiscono presidio di controllo sugli impatti ambientali.

A maggior garanzia delle aree a rischio, ulteriori presidi di controllo sono costituiti da:

- l'analisi degli specifici impatti ambientali derivanti dalle attività previste in Azienda e dall'organizzazione delle attività in Filiale;
- l'individuazione di un idoneo programma di misure atte a garantire la prevenzione dell'inquinamento e la diminuzione dei principali impatti ambientali;
- l'adeguata formazione del personale in materia ambientale e prescrizioni di legge e sulle misure di prevenzione degli impatti ambientali adottate in Azienda;
- il controllo costante circa la validità ed efficienza delle autorizzazioni connesse con la compatibilità ambientale delle attività svolte dalla Società;
- la verifica da parte di tutte le funzioni produttrici di rifiuti, le quali provvederanno a svolgere le seguenti attività:

    - individuazione delle tipologie dei rifiuti prodotti
    - deposito temporaneo dei rifiuti
    - affidamento dei rifiuti a ditte autorizzate al trasporto e allo smaltimento

- verifica della corretta compilazione dei formulari di trasporto
- verifica corretto aggiornamento dei registri di carico e scarico.

- la definizione delle modalità amministrative per il conferimento dei rifiuti alle società di raccolta e smaltimento, per le quali sia stata accertata la dotazione delle necessarie autorizzazioni di legge e, pertanto, inserite all'interno dell'albo fornitori;
- la tenuta di un registro nel quale annotare cronologicamente eventuali incidenti verificatisi che abbiamo comportato significativi impatti ambientali.

In occasione della valutazione degli aspetti ambientali e nei casi in cui si verifichino importanti modificazioni interne o esterne all'azienda, è necessario che il Responsabile Ambientale provveda a reperire tutti i dati necessari alla valutazione eseguendo un'analisi ambientale del sito interessato. In particolare l'analisi ambientale prevede, oltre all'identificazione e valutazione degli aspetti ambientali significativi:

- l'individuazione di tutte le prescrizioni di legge e di regolamento che possono interessare l'azienda;
- l'esame delle procedure e delle prassi consolidate in campo ambientale esistenti all'interno dell'azienda;
- l'analisi degli incidenti accaduti che hanno avuto conseguenze di tipo ambientale. Il RA deve garantire la rintracciabilità dei dati relativi all'analisi ambientale. In particolare, in fase di identificazione degli aspetti ambientali si definiscono le condizioni in cui si verifica ciascun impatto (normali/anomale o di emergenza). Al fine di assicurare la massima oggettività possibile, la valutazione degli aspetti ambientali significativi avviene considerando i seguenti parametri:
    - magnitudo dell'impatto ambientale generato;
    - frequenza di accadimento dell'impatto;
    - presenza di prescrizioni legali specifiche per l'aspetto considerato;
    - considerazione dell'aspetto nei principi d'azione della Politica Ambientale;
    - manifestazione d'interesse da parte di terzi;
    - grado di controllo esercitato sull'aspetto/impatto;
    - margine di miglioramento dell'aspetto ambientale.

A ciascuno di questi parametri è assegnato un punteggio che contribuisce a determinare il livello di significatività dell'aspetto. Sulla base dei valori del livello di significatività vengono quindi distinti gli aspetti ambientali significativi i quali permettono di definire le aree di maggiore interesse per la gestione ambientale.

8. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Al fine di verificare il processo in oggetto, i Responsabili degli Uffici interessati e, più in generale, i soggetti muniti di poteri in base al sistema di deleghe e procure sono tenuti a inviare, con periodicità definita dall'Organismo di Vigilanza, adeguati flussi informativi. Conformemente a quanto stabilito nella Parte Generale, fermo restando il suo potere discrezionale di attivarsi con specifici controlli di propria iniziativa o a seguito delle segnalazioni ricevute, l'OdV effettua periodicamente controlli a

campione sulle attività di "Gestione degli adempimenti previsti in materi di sicurezza, salute sul lavoro e ambiente", diretti a verificarne l'esplicazione in conformità.

9. CONSERVAZIONE DELLA DOCUMENTAZIONE

Tutta la documentazione (elettronica e cartacea) prodotta nell'ambito delle attività disciplinate nella presente procedura, è conservata a cura della Direzione e messa a disposizione su richiesta del Presidente del CdA, del Consiglio di Amministrazione e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

GESTIONE DELLA TESORERIA, DELLA FORMAZIONE DEL BILANCIO E DEI RAPPORTI CON I SOCI E CON GLI ORGANI DI CONTROLLO

INDICE

1. FINALITÀ 2

2. IL SISTEMA DEI CONTROLLI 2

2.1. STANDARD DI CONTROLLO GENERALI 2
2.2. STANDARD DI CONTROLLO SPECIFICI 3

3. AMBITO DI APPLICAZIONE 4

4. NORMATIVA DI RIFERIMENTO 4

5. REATI ASTRATTAMENTE PERPETRABILI 5

6. REGOLE GENERALI DI COMPORTAMENTO 14

7. PRESIDI DI CONTROLLO 15

7.1 MODALITÀ OPERATIVE DI GESTIONE DELLA TESORERIA 15
7.2 FORMAZIONE DEL BILANCIO CIVILISTICO 16
7.3 GESTIONE DEI RAPPORTI CON I SOCI E CON IL SINDACO UNICO 18

7. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA 19

8. CONSERVAZIONE DELLA DOCUMENTAZIONE 19

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il personale deve attenersi nell'ambito del processo di "**Gestione della tesoreria, della formazione del Bilancio e dei rapporti con i soci e con gli organi di controllo**".

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi Sociali, i Dipendenti, i Collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;
- Fornire all'OdV e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali , dei Dipendenti –in via diretta – dei Collaboratori Esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione – di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da - considerati individualmente o collettivamente - integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, nonché delle "*best practice*" prevede con riferimento alle Aree alle Attività Sensibili individuate:

- *standard di controllo "generali"*, applicabili a tutte le Attività Sensibili;
- *standard di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

2.1. STANDARDDI CONTROLLO GENERALI

Gli *standard* di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:

- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di

qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;

- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa- Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

2.2. STANDARD DI CONTROLLO SPECIFICI

Sulla base degli *standard* di controllo generali sopra riportati, gli *standard* di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;
b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
c) per tutte le operazioni:
   - siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
   - siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;
   - la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema

delle deleghe e procure;

- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

3. AMBITO DI APPLICAZIONE

Il presente Protocollo si applica a Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 e concerne, in particolare, tutte quelle funzioni/uffici interessati e coinvolti nei seguenti processi:

- apertura e chiusura dei conti correnti;
- gestione delle riconciliazioni bancarie;
- rilevazione e elaborazione delle informazioni contabili necessarie alla corretta e completa effettuazione delle chiusure contabili e alla redazione del bilancio civilistico della nota integrativa e di ogni altro documento previsto dalla legge o dallo statuto come necessario all'adozione della delibera di approvazione del Bilancio;
- gestione dei rapporti con Soci e con il Sindaco Unico.

Le Funzioni/servizi/uffici aziendali coinvolti nelle attività sensibili sono:

- Presidente del CdA;
- Consiglio di Amministrazione;
- Amministratori Delegati;
- Direzione Commerciale;
- Direzione Amministrazione, Finanza e Controllo Corporate;
- Responsabile Ufficio Legale Corporate;
- Responsabile Controllo e Recupero crediti;
- Ufficio Controlling;
- Ufficio Fatturazione;
- Ufficio Recupero crediti.

4. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30"*;

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;

- Protocollo sulla "Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità";
- Protocollo sulla "Gestione delle operazioni e degli adempimenti fiscali";
- Codice Etico del Gruppo Battistolli;
- Procedure e istruzioni operative;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Manuale di gestione del *software* di contabilità in uso;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

5. REATI ASTRATTAMENTE PERPETRABILI

I reati presupposto (nella forma consumata o tentata) di cui al D.lgs. 231/01 da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati.

- **Reati societari, introdotti dal D.lgs. 61/2002 e modificati dalla legge 262/2005 (art. 25-*ter*):**
  - False comunicazioni sociali (art. 2621 c.c.), False comunicazioni sociali. Fatto di lieve entità (art. 2621-*bis* c.c.), False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);

Nel nuovo articolo 2621 c.c, la condotta illecita consiste nell'esporre consapevolmente fatti materiali rilevanti non rispondenti al vero od omettere consapevolmente fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo a indurre altri in errore; per il reato è confermata la procedibilità d'ufficio (salvo nelle ipotesi in cui il fatto sia di lieve entità). L'articolo 2621-bis disciplina l'ipotesi che il falso in bilancio di cui all'articolo 2621 sia costituito da fatti "di lieve entità", salvo che costituiscano più grave reato. Tale fattispecie viene qualificata dal giudice tenendo conto: della natura e delle dimensioni della società e delle modalità o degli effetti della condotta. L'articolo 11 della legge 69/2015 modifica anche l'articolo 2622 del codice civile. I soggetti attivi del reato sono gli stessi di quelli individuati nella precedente versione dell'articolo 2622 ovvero amministratori, direttori generali, dirigenti addetti alla predisposizione delle scritture contabili, sindaci e liquidatori, con la differenza che qui si tratta di ruoli ricoperti in società quotate. La condotta illecita per il falso in bilancio nelle società quotate consiste nell'esporre consapevolmente fatti materiali non rispondenti al vero ovvero omettere fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene in modo concretamente idoneo a indurre altri in errore sulla situazione economica della società. Per la responsabilità amministrativa delle società, l'articolo 12 modifica l'articolo 25-ter del decreto legislativo 231 del 2001 (responsabilità amministrativa delle persone giuridiche), il quale reca una disciplina dei criteri di imputazione della responsabilità degli enti valevole per i reati societari. La disposizione interviene sui criteri soggettivi d'imputazione della responsabilità e sull'applicazione delle sanzioni pecuniarie alle società (per quote). La norma, nella formulazione prima vigente, limitava per i reati societari la cerchia dei possibili autori del fatto a soggetti che ricoprono specifici ruoli nella compagine organizzativa dell'ente (amministratori, direttori generali, liquidatori o persone sottoposte alla loro vigilanza). Tale limitazione viene ora superata dalla soppressione del riferimento ai citati ruoli di vertice.

Esempio: Vengono inserite in contabilità delle fatture di consulenze, false perché fondate su operazioni inesistenti ed effettuate al solo scopo di aumentare i ricavi della società.

Al fine di contrastare la realizzazione di tale fattispecie di reato è previsto apposito presidio di controllo "7.2 Formazione del bilancio civilistico" che, tramite l'utilizzo di un software professionale, garantisce la piena tracciabilità dell'operazione di carico dei dati e/o di modifica delle poste, prevedendo che ogni operazione sia sempre imputabile a un singolo operatore e che sia dotato delle necessarie autorizzazioni.

- Impedito controllo (art. 2625, comma 2, c.c.);

Il reato d'impedito controllo si verifica nell'ipotesi in cui, attraverso l'occultamento di documenti o altri artifici atti allo scopo, si impedisca o semplicemente si ostacoli lo svolgimento delle attività di controllo, che siano attribuite ai soci, ad altri organi sociali, dalla legge.

Esempio: L'amministratore della Società decide di trasferire i libri sociali dalla sede principale ad una sede periferica con l'intento di impedirne il controllo.

- Formazione fittizia del capitale (art. 2632 c.c.);

Tale ipotesi di reato è integrata dalle seguenti condotte: formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale; sottoscrizione reciproca di azioni o quote; sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione. Soggetti attivi del reato sono gli amministratori ed i soci conferenti.

- Indebita restituzione dei conferimenti (art. 2626 c.c.);

Il reato d'indebita restituzione dei conferimenti, previsto a tutela dell'integrità ed effettività del capitale sociale, quale garanzia dei diritti dei creditori e dei terzi, si verifica nel caso di restituzione, più o meno palese, dei conferimenti ai soci, ovvero nella liberazione degli stessi dall'obbligo di eseguirli, fuori dalle ipotesi di legittima riduzione del capitale sociale.

- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);

Il reato si realizza in due ipotesi. In primo luogo, nel caso in cui si ripartiscano utili, o acconti sugli utili, che non siano stati effettivamente conseguiti, o che siano destinati per legge a riserva. Si tratta dei cosiddetti utili fittizi, ossia utili che non risultano da operazioni concluse e da situazioni giuridiche definite ma incidono sul capitale sociale, traducendosi, in tal modo, in un illecito rimborso ai soci di conferimenti dagli stessi effettuati. L'altra ipotesi è quella in cui si ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite. Tuttavia, qualora gli utili siano restituiti, o le riserve ricostituite, prima del termine per l'approvazione del bilancio, il reato si estingue.

- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);

Il reato in oggetto si perfeziona con l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante, in modo tale da procurare una lesione all'integrità del capitale sociale e delle riserve non distribuibili per legge. Tuttavia, la ricostituzione del capitale sociale o delle riserve prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio nel corso del quale è stata posta in essere la condotta, estingue il reato.

- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);

Il reato si realizza nell'ipotesi in cui si proceda a riduzioni del capitale sociale, a fusioni con altra società ovvero a scissioni della società stessa, in violazione delle disposizioni previste dalla legge a tutela dei creditori. Perché il reato sussista, tuttavia, è necessario che da tali operazioni derivi un pregiudizio ai creditori; il reato si estingue qualora i creditori danneggiati siano risarciti prima del giudizio.

Esempio: La società effettua fusioni o scissioni con altre società, prima che siano trascorsi i 60 giorni previsti dall'art. 2503 c.c. o comunque in violazione delle disposizioni poste a tutela dei creditori: consenso preventivo, pagamento dei dissenzienti, deposito a garanzia.

- Omessa comunicazione del conflitto di interessi (art. 2629-*bis* c.c.);

Tale fattispecie di reato prevede la violazione di precetti, contemplati nella norma civilistica di riferimento e rivolti a taluni soggetti, dalla quale derivano «danni alla società o a terzi», da ritenersi di natura patrimoniale. Pertanto l'interesse protetto dalla norma è il patrimonio della società o dei terzi, in armonia con i principi ispiratori del nuovo sistema penale societario. Più in specifico, la norma rimanda all'art. 2391 c.c., primo comma, che impone ai membri del consiglio di amministrazione di comunicare (agli altri membri del consiglio e ai sindaci) ogni interesse che i medesimi, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata. L'amministratore delegato che sia portatore di un interesse in una determinata operazione della società deve astenersi dalla stessa, rimettendola alle determinazioni dell'intero consiglio. In entrambi i casi, la deliberazione del consiglio di amministrazione deve adeguatamente motivare le ragioni e la convenienza dell'operazione. È un reato proprio.

- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);

Il reato si consuma nell'ipotesi in cui i liquidatori procedano alla ripartizione tra i soci di beni sociali, senza aver provveduto al pagamento dei creditori della società, ovvero all'accantonamento delle somme necessarie a soddisfarli. Tuttavia, il reato sussiste unicamente se dalla condotta descritta derivi un danno ai creditori, e si estingue qualora il pregiudizio subito da questi ultimi sia risarcito prima del giudizio.

- Illecita influenza sull'assemblea (art. 2636 c.c.);

Il reato si perfeziona attraverso il compimento di atti simulati o fraudolenti, da chiunque posti in essere e a prescindere dalla finalità perseguita, che abbiano quale effetto la formazione di una maggioranza artificiosa all'interno dell'assemblea sociale. La prima condotta vietata dalla norma è quella della divulgazione, ossia della comunicazione ad un numero indeterminato di persone, di fatti materiali non rispondenti al vero; la seconda è invece integrata dal compimento di operazioni simulate. Da ultimo, la condotta criminosa può consistere nella predisposizione di artifici di vario genere purcheè idonei a conseguire l'effetto vietato dalla norma.

Esempio: Vengono ammessi al voto soggetti non aventi diritto, perche´ in conflitto di interesse con la delibera in votazione; oppure viene falsificato il numero degli intervenuti in assemblea.

- Aggiotaggio (art. 2637 c.c.);

L'art. 2637, mentre prima sanzionava il reato di aggiotaggio commesso in relazione a strumenti finanziari quotati e non quotati, oggi si applica ai soli casi di aggiotaggio posti in essere rispetto a «strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato». Nel caso di strumenti finanziari quotati si applicano, invece, le norme del TUF.

- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Il reato può realizzarsi in due diverse ipotesi. In primo luogo, nel caso in cui determinati soggetti (amministratori, direttori generali, sindaci, liquidatori di società o enti e, in generale, i soggetti sottoposti alle autorità pubbliche di vigilanza *ex lege*) espongano, in occasione di comunicazioni alle autorità pubbliche di vigilanza, cui sono tenuti in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che erano tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi. In tale prima ipotesi, il reato si perfeziona nel caso in cui la condotta criminosa sia specificamente volta ad ostacolare l'attività delle autorità pubbliche di vigilanza. La seconda ipotesi si realizza, invece, indipendentemente dal fine perseguito dagli stessi soggetti, ma soltanto qualora l'attività dell'autorità di pubblica vigilanza sia effettivamente ostacolata dalla loro condotta, di qualunque genere essa sia, anche omissiva.

- **Reati in materia di ricettazione, riciclaggio e impiego di denaro di provenienza illecita, introdotti dal D.lgs. 231/2007 (art. 25-*octies*):**

  - Ricettazione (art. 648 c.p.);

L'incipit della norma, in relazione al soggetto attivo, esclude che possa essere autore della ricettazione colui che ha commesso il reato da cui i beni provengono. Dunque chi commissiona il delitto presupposto concorre nella sua realizzazione come istigatore ed è punibile a tale titolo, mentre la successiva condotta di ricezione rileva come mero post factum non punibile. L'oggetto materiale è costituito da denaro o cose provenienti da delitto. La giurisprudenza vi comprende i servizi, l'energia o programmi di *know how*, mentre si divide riguardo gli immobili. Infine, riguardo ai rapporti con le figure concorrenti, si può tendenzialmente affermare che la ricettazione è destinata a lasciare spazio alle previsioni che incriminano specificamente la ricezione di un determinato bene di origine illecita. Ad esempio, in applicazione del principio di specialità *ex* art. 15 c.p., gli artt. 453, n. 3/4 e 455 c.p., che sanzionano chi acquista, riceve o detiene monete contraffate o alterate al fine di metterle in circolazione, sono destinati a prevalere sull'art. 648 c.p.

  - Riciclaggio (art. 648-*bis* c.p.);

Anche ai fini della configurabilità del reato di riciclaggio è necessario che sia in precedenza consumata altra fattispecie criminale. Più precisamente, affinché vi sia un provento illecito da riciclare – sia esso denaro o altro bene o utilità – è imprescindibile il fatto che un reato, per l'appunto presupposto sia stato commesso. Il riciclaggio consiste, quindi, nelle attività volte a dissimulare l'origine illecita dei proventi criminali ed a creare l'apparenza che la loro origine sia lecita.

  - Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);

Chi impiega denaro di provenienza delittuosa, direttamente in un'attività economica o finanziaria, così ripulendolo, risponde non del reato di riciclaggio, ma di quello punito dall'art. 648-ter c.p. appunto «Impiego di denaro, beni o utilità di provenienza illecita». In quest'ultimo, infatti, è "assorbita" la precedente attività di sostituzione o di ricezione. Invece, se taluno sostituisce denaro di provenienza illecita con altro denaro o altre unità e, poi, impieghi i proventi derivanti da tale opera di ripulitura in attività economiche o finanziarie, risponde del solo reato di riciclaggio (art. 648 bis c.p.) con esclusione del 648-ter c.p.

- Autoriciclaggio (art. 648-*ter*1 c.p.).

Il delitto di riciclaggio, così come formulato dall'art. 648- bis c.p., punisce chi ricicla denaro, beni o altre utilità provenienti da un delitto non colposo commesso da un altro soggetto, mentre nessuna sanzione era prevista per chi ricicla in prima persona , cioè sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo da egli commesso (o che ha concorso a commettere), ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. L'introduzione del reato di autoriciclaggio è stata necessaria per colmare questa lacuna nel nostro ordinamento. Il delitto di autoriciclaggio, peraltro, prevede pene diverse a seconda della gravità del delitto presupposto e con previsione della non punibilità delle condotte nelle quali il denaro, i beni o le altre utilità vengono destinati «alla mera utilizzazione o al godimento personale».

- **Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, introdotti dal D.Lgs. 184/2021 e modificati dalla L. n. 137/2023 (art. 25 octies I):**

  - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter, co. I c.p.).

Il delitto di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, così come formulato dall'art. 493 ter, co. I c.p., punisce chi indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti. La norma contempla, altresì, l'ipotesi del soggetto che falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. La novella del legislatore estende il campo della condotta, contemplando ogni strumento di pagamento diverso dal contante che sia idoneo ad abilitare al prelievo del denaro o all'acquisto di beni o prestazione di servizi o comunque rappresenti uno strumento di pagamento diverso dal contante.

  - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater, co. I c.p.).

La norma contempla l'ipotesi in cui, salvo che il fatto costituisca più grave reato, il soggetto che, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

  - Frode informatica (640 ter, co. I c.p.).

Il delitto di frode informatica, così come formulato dall'art. 640 ter, co. I c.p., punisce chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. La norma prevede, peraltro, pene diverse a seconda che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale o sia commesso con abuso della qualità di operatore del sistema dall'ipotesi, più grave, in cui il fatto sia commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

- Trasferimento fraudolento di valori (art. 512 *bis* c.p.)

Tale fattispecie punisce, salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648 bis, e 648 ter. Con l'inserimento della presente norma il legislatore ha inteso sanzionare penalmente la condotta fraudolenta di chi trasferisca fittiziamente ad altri denaro od altri beni al fine di elidere l'applicazione delle disposizioni in materia di mezzi di prevenzione patrimoniale, contrabbando ovvero al fine di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio. Tale fattispecie è volta a coprire la condotta di chi non trasferisca effettivamente la titolarità dei beni o del denaro, ma lo faccia fittiziamente, continuando dunque ad avere la disponibilità materiale degli stessi e continuando dunque a goderne.

- **Delitti di criminalità organizzata, introdotti dalla Legge 94/2009 (art. 24-*ter*):**
  - Associazione per delinquere, anche diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-*bis*, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286 (art 416 c.p.);

I delitti associativi in generale hanno carattere plurisoggettivo, ossia richiedono la partecipazione di almeno tre persone. La partecipazione può essere anche di secondaria importanza, purché il contributo sia apprezzabile, concreto e dotato di effettiva stabilità.Ai fini della configurabilità del delitto di associazione per delinquere, è necessaria la predisposizione di un'organizzazione strutturale, sia pure minima, di uomini e mezzi, funzionale alla realizzazione di una serie indeterminata di delitti, nella consapevolezza, da parte dei singoli associati, di far parte di un sodalizio durevole e di essere disponibili ad operare per l'attuazione del programma criminoso comune. In altre parole, l'art. 416 c.p. punisce coloro che promuovono, costituiscono o organizzano l'associazione allo scopo di commettere più delitti. Anche il solo fatto di partecipare all'associazione costituisce reato. La rilevanza penale delle condotte descritte dalla norma appare condizionata all'effettiva costituzione dell'associazione criminosa. Infatti, prima ancora di richiamare le singole condotte di promozione, costituzione, direzione, organizzazione ovvero di semplice partecipazione, la norma ne subordina la punibilità al momento in cui «tre o più persone» si siano effettivamente associate per commettere più delitti. Il delitto di associazione per delinquere si caratterizza quindi per l'autonomia dell'incriminazione rispetto agli eventuali reati successivamente commessi in attuazione del *pactum sceleris*. Tali eventuali delitti, infatti, concorrono con quello di associazione per delinquere e, se non perpetrati, lasciano sussistere il delitto previsto dall'art. 416 c.p. Al netto delle considerazioni sopra svolte, la configurazione dei reati associativi come reati-mezzo ha l'effetto di estendere la responsabilità dell'ente ex decreto 231 a una serie indefinita di fattispecie criminose commesse in attuazione del *pactum sceleris* e non necessariamente incluse nell'elenco dei reati presupposto.

- **Reati contro la Pubblica Amministrazione (artt. 24 e 25):**
  - Corruzione tra privati (art. 2635 c.c.);

La nuova formulazione dell'art. 2635 c.c. estende il novero dei soggetti attivi includendo tra gli autori del reato, oltre a coloro che rivestono posizioni apicali di amministrazione o di controllo, anche coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive presso società o enti privati. Ai fini "231", per quanto concerne la corruzione tra privati, resta reato-presupposto la sola fattispecie di cui al comma 3 dell'articolo 2635 del codice civile, cioè il delitto commesso da chi corrompe, oggi anche per interposta persona, i soggetti indicati nel primo comma del medesimo articolo (nella sua nuova e più estesa versione) per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

- Istigazione alla corruzione tra privati (art. 2635 bis c.c.)

Diventa invece nuovo reato-presupposto anche l'istigazione alla corruzione tra privati (nuovo articolo 2635-bis comma 1). Anche in questo caso solo a carico della società alla quale appartiene il soggetto che istiga alla corruzione gli esponenti aziendali altrui, per avvantaggiare la propria società di appartenenza. Novità assoluta: si applicano sia alla corruzione tra privati sia all'istigazione le sanzioni interdittive previste dall'art 9, comma 2, del D.lgs. 231/01.

- Truffa in danno dello Stato o di un ente pubblico (art. 640, comma 2, n. 1, c.p.).

Il reato di concussione si caratterizza per l'utilizzo indebito da parte del funzionario pubblico dei propri poteri, al fine di costringere il soggetto passivo a riconoscere al funzionario o ad un terzo soggetto un vantaggio di natura economica o personale. Si ha abuso dei poteri quando gli stessi siano esercitati fuori dei casi previsti da leggi, regolamenti e istruzioni di servizio o senza le forme prescritte, ovvero quando detti poteri, pur rientrando tra quelli attribuiti al pubblico ufficiale, vengano utilizzati per il raggiungimento di scopi illeciti.

- **Reati di abuso di informazioni privilegiate e di manipolazione del mercato, introdotti dalla legge 62/2005 (art. 25-*sexies*):**
  - Abuso di informazioni privilegiate (art. 184 D.lgs. 58/1998);

L'abuso di informazione privilegiate (o *Insider Trading*), consiste nella situazione per la quale un soggetto investitore (*Insider primario*) in possesso di un'informazione privilegiata, non ancora resa nota al pubblico ed in grado di avere effetti diretti sul prezzo di uno strumento finanziario, la sfrutta a proprio vantaggio, oppure decide di comunicarla ad altri investitori (*Insider secondari*) o addirittura di raccomandare determinati investimenti sfruttando il suddetto vantaggio informativo (attività c.d. *Tipping* e *Tuyayutage*).

  - Manipolazione del mercato (art. 185 D.lgs. 58/1998).

La manipolazione del mercato consiste, invece, nella diffusione di notizie false o tendenziose ma apparentemente degne di credito, al fine di alterare il prezzo degli strumenti finanziari.

- **Reati tributari, introdotti dalla L. n. 157/2019 (art. 25-quinquiesdecies):**
  - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. n. 74/2000);

L'art. 2 del D.lgs 74/2000 prevede che sia punito chiunque al fine di evadere le imposte sui redditi e l'Iva indica in una dichiarazione elementi passivi fittizi attraverso fatture o altri documenti per operazioni inesistenti. Seconda consolidata giurisprudenza, integra il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, la falsa indicazione, nella dichiarazione Irpef, di spese deducibili dall'imposta, quando le stesse non siano state effettuate o siano state effettuate in misura inferiore. (cfr.Cass. civ., n. 48486/2011 e 27392/2012). In relazione al mezzo fraudolento di cui l'agente si avvale per l'indicazione in dichiarazione di elementi passivi fittizi, la Corte di cassazione ha fornito, una definizione degli altri documenti rilevanti ai sensi dell'art. 2 del d.lgs. n. 74/2000, precisando che tali sono quelli «[…] aventi, ai fini fiscali, valore probatorio analogo alle fatture (documenti tipici fiscali previsti espressamente dal d.P.R. 633/1972, art. 21)». Pertanto, può dirsi che ai fini della sussistenza del reato di dichiarazione fraudolenta di cui all'art. 2 del d.lgs. 74/2000, per fatture o altri documenti per operazioni inesistenti devono intendersi quelli che, a prescindere dal *nomen*, hanno l'attitudine, in base alle norme dell'ordinamento tributario, a fornire la prova delle operazioni in essi documentati. A tal fine non è necessario stabilire *ex post* se il documento possa avere tale attitudine ma è sufficiente che, per le sue caratteristiche estrinseche e per il suo contenuto, tale natura non possa essere esclusa *ictu oculi* in base alle norme dell'ordinamento tributario sin dalla fase dell'accertamento fiscale (Cassazione penale sez. III, 27/02/2018, n.40448).

- Dichiarazione fraudolenta mediante altri artifici (art.3 D.lgs n. 74/2000)

La dichiarazione fraudolenta potrà essere realizzata, oltre che con le modalità previste dall'articolo precedente, anche con l'utilizzo di altri artifizi. Quest'ultima è costruita, essenzialmente, come frode contabile, alla quale deve associarsi un *quid pluris* artificioso non tipizzato (diverso dall'uso di fatture o altri documenti falsi, integrante l'ipotesi di cui al precedente art. 2) ma, comunque, caratterizzato dall'idoneità a indurre in errore e a impedire il corretto accertamento della realtà contabile del soggetto che presenta la dichiarazione annuale d'imposta, come:la tenuta di un sistema parallelo di contabilità "nera"; la vendita "a nero" organizzata in locali contigui a quelli del Fondo; la voluta "confusione" di ricavi provenienti da fonti diverse in modo da impedire di individuare il titolare degli stessi; lo spostamento artificioso di redditi tra soggetti rivolto a fare figurare come percepiti da terzi redditi propri del contribuente.

- Dichiarazione infedele (art. 4 D. Lgs. n. 74/2000)

Fuori dei casi previsti dagli articoli 2 e 3, è punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.
La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).

- Omessa dichiarazione (art. 5 D.lgs. n. 74/2000)

È punito chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila. La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).

- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs n. 74/2000)

L'art. 8 del D.lgs n. 74/2000 punisce chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.La realizzazione della condotta *de qua* necessita che la fattura o il documento escano dalla sfera di fatto e di diritto dell'emittente mediante consegna o spedizione a un terzo potenziale utilizzatore, che non abbia partecipato alla perpetrazione del falso. La condotta delittuosa in esame, si pone all'inizio di un percorso che porterà, nella maggior parte dei casi, all'utilizzo di tali documenti e quindi al concretizzarsi del reato di cui all'art. 2 – dichiarazione fraudolenta - realizzando appieno quel *fine di consentire a terzi l'evasione*. Sono reati legati dall'unicità del fine, nel senso che il primo (art. 8) costituisce il mezzo normale per realizzare il secondo (art. 2).

- Occultamento o distruzione di documenti contabili (art. 10 D.lgs n. 74/2000)

L'art. 10 del D.lgs n. 74/2000 prevede la reclusione per chiunque, al fine di evadere le imposte sui redditi e l'Iva, ovvero consentire l'evasione a terzi, occulta o distrugge le scritture contabili o i documenti di cui è obbligatoria la conservazione. Secondo la giurisprudenza, ai fini della configurazione del reato, non è sufficiente un mero comportamento omissiovo, ossia la omessa tenuta delle scritture contabili, che renda obiettivamente più difficoltosa -ma non impossibile- la ricostruzione della situazione contabile ma è necessario un "quid pluris" a contenuto commissivo consistente nell'occultamento o nella distruzione dei documenti contabili la cui istituzione e tenuta è obbligatoria per legge (Cass. Pen., Sez. 3, n. 19106 del 02/03/2016).

- Indebita compensazione (art. 10 *quater* D. Lgs. n. 74/2000)

È punito chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro. È punito chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro. **La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).**

- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.lgs n. 74/2000)

Nella nozione di atti fraudolenti, rilevante ai fini della configurabilità del delitto di sottrazione fraudolenta al pagamento delle imposte, rientrano tutti quei comportamenti che, anche se formalmente leciti, risultino connotati da elementi di inganno o di artificio dovendosi ravvisare l'esistenza di uno stratagemma tendente a sottrarre le garanzie patrimoniali all'esecuzione. Tale reato si configura, sotto il profilo oggettivo, sia mediante una vendita simulata sia attraverso il compimento di altri atti fraudolenti. Secondo la previsione normativa questi ultimi debbono essere «idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva». E ciò anche in aderenza all'interesse protetto dalla norma a rendere possibile la riscossione nei confronti del contribuente (bene giuridico peraltro protetto a livello costituzionale dall'art. 53 Cost.). La Suprema Corte, ha affermato, in materia di sottrazione fraudolenta, che: la natura : «la natura fraudolenta degli atti dispositivi presuppone non soltanto la lesione di un diritto altrui, per effetto della riduzione del patrimonio del debitore che rende più difficoltosa l'azione di recupero dell'erario, ma anche che il pregiudizio arrecato non sia immediatamente percepibile»(Cass. pen., Sez. III, 16 maggio 2017,n. 10161). Deve, invece, rilevarsi come per vendita simulata debba intendersi una «alienazione finalizzata a creare una situazione giuridica apparentemente diversa da quella reale, sicché l'alienazione è simulata quando il programma contrattuale non corrisponde deliberatamente in tutto (simulazione assoluta) o in parte (simulazione relativa) alla effettiva volontà dei contraenti» (Cass. pen., Sez. III, 5 luglio 2016, n. 3011); ancora, il negozio può essere simulato sotto il profilo "oggettivo" o "soggettivo" a seconda che gli artifici riguardino gli elementi afferenti il bene compravenduto ovvero le parti che vi sono coinvolte (*ex plurimis*Cass.pen., Sez. III, 06 marzo 2008, n. 14720).

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

6. REGOLE GENERALI DI COMPORTAMENTO

La gestione della contabilità e della tesoreria, coerentemente con i principi enunciati nell'ambito del Codice Etico, deve essere realizzata in modo che tutte le transazioni effettuate su conti correnti in essere siano evidenziate in apposite registrazioni su archivi informatici e sempre corrispondenti a flussi che siano riferibili a poste di bilancio correttamente rappresentate.

Nell'ambito della formazione del bilancio e gestione dei rapporti con gli Organi di Controllo, il personale deve fare riferimento alle seguenti modalità operative:

- nella gestione delle attività contabili devono essere osservate scrupolosamente le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla legge e dai principi contabili nazionali o internazionali applicabili, in modo tale che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto ed essere effettuata in conformità e coerenza con le Istruzioni Operative utilizzando esclusivamente il *software* dedicato. Pertanto, sarà compito della Direzione Amministrazione e Finanza per le funzioni a questi attribuite nell'ambito dell'organigramma aziendale assicurare che la documentazione di supporto sia facilmente reperibile e ordinata secondo criteri logici oltre che immediatamente disponibile per ogni eventuale attività di *audit* interno.

I dati vengono, altresì, sempre assunti esclusivamente tramite sistemi informatici in grado di verificare, per il ciclo passivo di fatturazione, la corrispondenza tra l'impegno di spesa assunto e il relativo impiego di risorse; per il ciclo attivo, la piena corrispondenza tra le effettive prestazioni erogate, il valore delle stesse e le richieste in pagamento rivolte ai soggetti pubblici/privati.

L'intero processo di acquisizione dei dati relativi alle poste contabili attive e passive viene realizzato dalla Società per il tramite di apposito *software*.

Eventuali operazioni straordinarie devono essere poste in essere nel rispetto della disciplina prevista dal Codice Civile.

Nello svolgimento delle attività di verifica e controllo da parte del Sindaco Unico, della società eventualmente incaricata della Revisione e dei Soci è necessario agire con trasparenza e prestare la massima collaborazione.

A titolo esemplificativo e non esaustivo, nell'ambito delle operazioni societarie non è consentito:

- porre in essere operazioni simulate o diffondere notizie false sulla Società e sulle sue attività;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in Bilancio, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- restituire conferimenti ai Soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Sindaco Unico;
- fare un utilizzo improprio degli strumenti di pagamento diversi dal contante;
- alterare, distrarre o mettere a disposizione d'altri gli strumenti di pagamento diversi dal contante;
- alterare i sistemi informatici al fine di modificare o alterare strumenti di pagamento diversi dal contante.

Ogni trasferimento di beni o altre utilità deve essere effettuato nel rispetto dell'operatività aziendale e in coerenza con le linee di indirizzo e le scelte strategiche definite dal CdA. In ogni caso, i soggetti aziendali (es. Amministratori, Procuratori, etc.) coinvolti (in qualità di alienante o acquirente) nel trasferimento di valori, largamente intesi, sono tenuti a verificare:

- l'identità della parte contraente nonché l'assenza di rapporti di parentela e affinità tra le parti;
- l'eventuale irrisorietà del prezzo pattuito, rispetto al valore effettivo;
- il mancato pagamento del prezzo concordato e la conseguente indisponibilità/mancata amministrazione dei valori;
- la sussistenza del patto di riscatto tra le clausole contrattuali.

La Direzione Amministrazione, Finanza e Controllo verifica, al momento della ricezione del relativo contratto, l'eventuale sussistenza di una delle condizioni di cui sopra, segnalando tempestivamente all'OdV, la tipologia di rapporto in essere nonché la condizione riscontrata nel rapporto contrattuale.

7. PRESIDI DI CONTROLLO

7.1 MODALITÀ OPERATIVE DI GESTIONE DELLA TESORERIA

7.1.1 APERTURA, GESTIONE E CHIUSURA DEI CONTI CORRENTI

L'autorizzazione all'apertura o alla chiusura di un conto corrente è di esclusiva competenza del Presidente e degli Amministratori e/o procuratori appositamente delegati.

Le attività operative di gestione (es. invio documentazione, comunicazioni, etc.) sono di competenza della Direzione Amministrazione, Finanza e Controlloo di altri soggetti formalmente delegati, e sono periodicamente monitorate dal Presidente del CdA, il quale richiede il dettaglio dei conti in essere e delle movimentazioni su di essi. Inoltre, il Direttore Amministrazione, Finanza e Controllo discute e negozia con cadenza periodica, anche in funzione delle esigenze e specifiche circostanze, le condizioni economiche (es. interessi, spese, commissioni, etc.) che regolano i rapporti di conto

corrente, nonché monitora la corretta applicazione delle stesse. Annualmente il Direttore Amministrazione, Finanza e Controllo accerta con gli Istituti bancari che i poteri di firma depositati siano aggiornati rispetto alle procure societarie e, nel caso di disallineamenti, comunica agli Istituti di effettuare le relative modifiche, trasmettendo la dovuta documentazione di supporto.

Tutti i pagamenti aziendali devono essere effettuati tramite meccanismi di tracciamento informatico (*home banking*), secondo il principio della doppia sottoscrizione.

La Società effettua quotidianamente il riscontro di cassa. La Direzione Amministrazione, Finanza e Controllo verifica che tutti i pagamenti siano dotati delle necessarie autorizzazioni.

7.1.2 GESTIONE DELLE RICONCILIAZIONI BANCARIE

Con cadenza periodica almeno mensile, la Direzione Amministrazione, Finanza e Controllo effettua la riconciliazione tra gli estratti conto bancari e la scheda contabile dei conti correnti.

In caso di disallineamenti nelle riconciliazioni, il Responsabile, dopo aver verificato la motivazione dello scostamento e archiviato idonea documentazione a supporto, riallinea la scheda contabile rispetto alle operazioni registrate nell'estratto conto bancario (tramite scritture di storno e conguaglio) o, viceversa, richiede alla banca la necessità di correggere eventuali errori od omissioni di registrazione in conto corrente.

Eventuali anomalie nelle riconciliazioni sono segnalate agli Organi di controllo nonché all'OdV.

7.1.3 GESTIONE DEI PAGAMENTI

Tutti i pagamenti vengono effettuati previa verifica dell'avvenuta autorizzazione da parte dei singoli soggetti titolari del potere di disporre spese. Il Direttore Amministrazione, Finanza e Controllo assicura che i pagamenti vengano disposti esclusivamente laddove il processo decisionale che porta alla richiesta di pagamento sia stato correttamente seguito da parte delle singole Funzioni che richiedono di procedere. Laddove riscontri eventuali criticità o difformità rispetto alla procedura, ne dà comunicazione al soggetto responsabile affinché fornisca spiegazioni e ne informa gli Organi di controllo, nonché l'OdV. Nel caso in cui la difformità o l'anomalia venga successivamente sanata, procede al pagamento, archiviando copia della corrispondenza intercorsa.

7.2 FORMAZIONE DEL BILANCIO CIVILISTICO

La contabilità generale è tenuta e gestita tramite *software* professionale dalla Direzione Amministrazione e Finanza.

La gestione della contabilità dovrà attenersi al manuale d'uso, garantendo la piena tracciabilità dell'operazione di carico dei dati e/o di modifica delle poste, al contempo prevedendo che ogni operazione sia sempre imputabile a un singolo operatore che sia dotato delle necessarie autorizzazioni.

In coerenza con le scadenze stabilite dalla legislazione italiana nell'ambito delle attività di predisposizione, approvazione e comunicazione del Bilancio Civilistico, la Direzione

Amministrazione e Finanza pianifica le attività necessarie alla chiusura dell'esercizio sociale e alla redazione del progetto di Bilancio.

Il processo di chiusura del Bilancio è verificato dal Direttore Amministrazione, Finanza e Controllo, il quale si occupa di:

- pianificare le attività necessarie alla chiusura dell'esercizio sociale e alla redazione del progetto di Bilancio;
- predisporre e inoltrare alle Funzioni coinvolte un calendario di chiusure contabili, in coerenza con le scadenze stabilite dalla legislazione italiana nell'ambito delle attività di predisposizione, approvazione e comunicazione del Bilancio Civilistico;
- monitorare i dati contabili presenti a sistema, analizzandoli su base comparativa rispetto ai periodi precedenti, e verificandone la congruità;
- verificare la tempestività, la completezza e la correttezza dell'esecuzione delle scritture automatiche generate a sistema (in base alle linee guida predefinite a sistema), es. ammortamenti;
- sollecitare l'inserimento o l'adeguamento automatico di alcune voci, al fine di giungere a una completezza dei dati contabili entro le tempistiche di chiusura previste;
- verificare le scritture di assestamento e di rettifica, nonché la determinazione delle poste valutative di Bilancio per la verifica degli aggiornamenti fiscali a essi connessi;
- accertarsi che sia dato tempestivo riscontro alla richiesta di dati e/o informazioni, segnando eventuali omissioni o ritardi non giustificati agli organi di controllo.

7.2.1 ANALISI DEL BILANCIO DI VERIFICA E CHIUSURA

Al termine delle operazioni di assestamento, è stampato un Bilancio di verifica sul quale il Direttore Amministrazione e Finanza esegue gli ultimi controlli di correttezza, completezza e coerenza delle scritture.

In caso di errori evidenziati sull'ultima versione del Bilancio di verifica, il Direttore Amministrazione e Finanza esegue direttamente le registrazioni correttive sul sistema di contabilità generale, dandone comunicazione agli Organi di controllo, nonché all'OdV. Dopo l'approvazione del Bilancio da parte dell'Assemblea dei Soci, non è più possibile eseguire sul sistema scritture contabili con impatto sull'esercizio precedente, che risulta definitivamente chiuso.

7.2.2. PREDISPOSIZIONE E APPROVAZIONE DEL PROSPETTO DI BILANCIO

Completate le operazioni di chiusura, il Direttore Amministrazione e Finanza si occupa della predisposizione del Prospetto di Bilancio, della Nota Integrativa e della Relazione sulla Gestione, nel rispetto delle normative vigenti in materia di informativa di bilancio.

Completate le operazioni di chiusura, il Direttore Amministrazione e Finanza si occupa della predisposizione del Prospetto di Bilancio, della Nota Integrativa e della Relazione sulla Gestione nel rispetto delle normative vigenti in materia di informativa di bilancio.

Successivamente il prospetto è inviato dal Direttore Amministrazione e Finanza ai singoli Amministratori e al Sindaco Unico, secondo i tempi previsti dalla normativa, affinché possano analizzarlo e avanzare eventuali eccezioni prima della riunione di approvazione.

Il Prospetto di Bilancio è dunque presentato, ai fini dell'approvazione, al Presidente del Consiglio di Amministrazione e discusso nel corso del Consiglio di Amministrazione, alla presenza del Sindaco Unico.

Il Bilancio, unitamente alla Nota Integrativa e alla Relazione sulla Gestione, aggiornato alla luce di eventuali modifiche richieste nel corso del Consiglio di Amministrazione, è presentato all'Assemblea dei Soci per l'approvazione finale secondo le modalità e i tempi previsti dalla normativa.

7.3 GESTIONE DEI RAPPORTI CON I SOCI E CON IL SINDACO UNICO

7.3.1 RAPPORTI CON I SOCI

Il Responsabile Ufficio Legale Corporate è il referente aziendale delegato ai rapporti con i Soci.

La Funzione Legale è responsabile di:

- predisporre le convocazioni delle Assemblee dei Soci;
- soddisfare in autonomia richieste di informazioni e chiarimenti "di ordinaria amministrazione" (es. relative allo statuto), anche attraverso, ove necessario, il coinvolgimento di personale interno alla Società, agendo nella massima correttezza e trasparenza;
- predisporre la documentazione in caso di richieste specifiche sottoposte dai Soci agli amministratori (es. trasferimenti azionari, iscrizione al Libro Soci, ecc.);
- mantenere traccia delle richieste di documentazione dei Soci e della relativa documentazione fornita;
- mettere a disposizione dei Soci, tramite anche strumenti o piattaforme informatiche che garantiscano la tracciabilità, tutta la documentazione necessaria all'adozione delle delibere assembleari, laddove previsto dallo Statuto e/odalla legge;
- fornire risposte in ordine all'andamento sociale e ogni altra informazione inerente la Società esclusivamente ai Soci tramite comunicazioni scritte o con posta elettronica tracciabile della Società, laddove previsto dallo Statuto e/o dalla Legge.

Gli Amministratori sono responsabili di operare con tempestività, trasparenza e nel più assoluto rispetto delle normative applicabili per consentire ai Soci e al Sindaco Unico di effettuare, nel rispetto dei tempi previsti, gli adempimenti loro riservati.

7.3.2 RAPPORTI CON IL SINDACO UNICO

Tutti gli Uffici forniscono supporto e informazioni al Sindaco Unico, attivandosi per:

- raccogliere la documentazione a supporto dell'attività del Sindaco Unico e soddisfare le richieste informative avanzate dallo stesso, agendo nella massima correttezza e trasparenza;
- archiviare la documentazione legata all'attività del Sindaco Unico;
- assistere il Sindaco Unico nel corso delle verifiche periodiche di merito (es. controllo libri sociali), quale interfaccia verso le strutture organizzative della Società.

7. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Al fine di verificare il processo in oggetto, i Responsabili delle Funzioni/Uffici interessati e, più in generale, i soggetti muniti di poteri in base al sistema di deleghe e procure sono tenuti ainviare, con periodicità definita dall'Organismo di Vigilanza, adeguati flussi informativi. Conformemente a quanto stabilito nella Parte Generale, fermo restando il suo potere discrezionale di attivarsi con specifici controlli di propria iniziativa o a seguito della segnalazione ricevute, l'OdV effettua periodicamente controlli a campione sulle attività di "Gestione della Tesoreria, della Formazione del Bilancio e dei rapporti con i Soci e con gli Organi di controllo", e comunque su ogni attività sensibile individuata nel presente Protocollo, diretti a verificarne l'applicazione in conformità a quanto sopra previsto.

8. CONSERVAZIONE DELLA DOCUMENTAZIONE

I Responsabili delle Funzioni/Uffici coinvolti nei processi sensibili individuati nel presente Protocollo operativo sono responsabili, ciascuno per la parte di propria competenza, della conservazione della documentazione, nel rispetto dei termini di legge, al fine di garantire la tracciabilità delle operazioni aziendali. La documentazione è, inoltre, messa a disposizione, su richiesta, del Consiglio di Amministrazione, del Sindaco Unico e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

GESTIONE DELLE INFRASTRUTTURE TECNOLOGICHE E DEI SISTEMI INFORMATIVI

INDICE

1. FINALITÀ 2

2. AMBITO DI APPLICAZIONE 2

2.1 Le attività a potenziale "rischio reato" 2
2.2 Le Funzioni aziendali coinvolte 2

3. NORMATIVA DI RIFERIMENTO 3

4. REATI ASTRATTAMENTI PERPETRABILI 3

5. REGOLE GENERALI DI COMPORTAMENTO 6

6. IL SISTEMA DEI CONTROLLI 8

7. PRESIDI DI CONTROLLO SPECIFICI 9

7.1 Gestione del profilo utente e del processo di autenticazione 9
7.2 gestione dei sistemi hardware e software 10
7.3 Uso della posta elettronica 10
7.4 Navigazione in internet 11
7.5 Gestione dei documenti informatici pubblici o privati aventi efficacia probatoria 12
7.6 Sicurezza dei sistemi informativi 13
7.7 installazione e gestione di sistemi di videosorveglianza 13
7.8 Software antiriciclaggio 14
7.9 Procedura di whistleblowing 14

8. LA TUTELA DEI DATI PERSONALI 15

9. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 16

10. CONSERVAZIONE DELLA DOCUMENTAZIONE 17

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il personale deve attenersi nell'ambito del processo di "**Gestione delle infrastrutture tecnologiche e dei sistemi informativi**".

Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società, nelle procedure e istruzioni operative, e nelle disposizioni interne aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi sociali, i dipendenti, i collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle altre Funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi sociali, dei dipendenti – in via diretta – e dei collaboratori esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione – di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da – considerati individualmente o collettivamente – integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. AMBITO DI APPLICAZIONE

2.1 LE ATTIVITÀ A POTENZIALE "RISCHIO REATO"

Il presente Protocollo si applica alla società Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 e concerne, in particolare, tutte quelle Funzioni e unità operative coinvolte nelle seguenti attività:

- Gestione del profilo utente e del processo di autenticazione;
- Gestione e protezione della postazione di lavoro;
- Gestione e protezione delle reti e sicurezza fisica dei sistemi informatici;
- Utilizzo della posta elettronica e della rete *Internet*;
- Gestione delle autorizzazioni e delle licenze di programmi *software* e banche dati;
- Invio telematico di atti, documenti e scritture;
- Installazione e gestione di sistemi di videosorveglianza.

2.2 LE FUNZIONI AZIENDALI COINVOLTE

Attesa la peculiarità e la trasversalità dei processi interessati dal Protocollo, esso si applica a tutti i

dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori della Società indipendentemente dal rapporto contrattuale con l'Azienda (lavoratori somministrati, collaboratori a progetto, in *stage*, ecc.), coinvolti nell'utilizzo di sistemi informativi ovvero infrastrutture tecnologiche.

La gestione operativa delle procedure è affidata all'Ufficio Sistemi Informativi, in coordinamento con il DPO nominato dalla Società per le questioni attinenti alla normativa sulla protezione dei dati personali e con il Responsabile Sistemi di Sicurezza e Innovazione.

Ai fini del presente Protocollo, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione.

3. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30*"
- Regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR);
- D.lgs. n. 101/2018 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679"*;
- D.lgs. n. 196/2003 *"Codice in materia di protezione dei dati personali"*;
- Legge 22 aprile 1941 n. 633 *"Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"* e ss.mm.ii.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;
- Codice Etico del Gruppo Battistolli;
- Regolamento aziendale per l'utilizzo del sistema informatico;
- Manuale Antiriciclaggio adottato dalla Società;
- Procedure e istruzioni operative;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Policy 8.1. - Whistleblowing;
- Manuale della protezione dei dati personali
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

4. REATI ASTRATTAMENTI PERPETRABILI

I reati presupposto (nella forma consumata o tentata) di cui al D.lgs. 231/01 da prevenire seguendo i controlli e attuando le procedure elaborate nel presente documento sono di seguito elencati.

- **Delitti informatici e trattamento illecito di dati, introdotti dalla legge 48/2008 (art. 24-*bis*):**
  - Accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.);

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Cass. 3067/1999). Il sistema informatico, dovendo svolgere una funzione - mediante tecnologie informatiche - è dunque tale se gestisce o elabora dati, mentre tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è "sistema informatico".
Dirimente ai fini della configurabilità del reato è la presenza o meno delle cd. misure di sicurezza nel sistema informatico / telematico. L'apposizione di siffatte misure protettive del sistema informatico o telematico costituisce, infatti, l'estrinsecazione della *voluntas excludendi* manifestata dal titolare del relativo *ius*.

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);

Tale norma mira a impedire l'intercettazione fraudolenta, ravvisabile ogniqualvolta l'agente prenda conoscenza delle comunicazioni in maniera occulta e senza essere legittimato.

- Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);

Tale norma è volta a sanzionare la semplice predisposizione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Esempio: Un amministratore o dipendente della società impedisce/interrompe una comunicazione al fine di ostacolare una società concorrente nell'invio della documentazione relativa ad una gara ovvero di materiale destinato alla clientela in modo da determinarne l'inadempimento.

Al fine di contrastare la realizzazione di tale fattispecie di reato, è previsto apposito presidio di controllo "7.2 Gestione dei sistemi Hardware e Software" che vieta l'installazione di qualunque software diverso da quelli autorizzati dalla Società e non pertinente allo scopo per cui il sistema informatico è stato assegnato all'utente. Espressamente vieta, inoltre, qualsiasi modifica delle configurazioni impostate sul proprio pc o dispositivo aziendale, mantenendo traccia delle citate modifiche e consentendo l'apposita attività di verifica.

- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);

L'art. 635-bis non si limita ad ampliare ed integrare la norma sul danneggiamento (art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispone altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilo sanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali: il sistema informatico o telematico, ovvero il supporto materiale delle informazioni. Il danneggiamento si può attuare nella distruzione e nel deterioramento e nell'inservibilità totale o parziale.

- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-ter c.p.);

L'art.635 ter è volto a sanzionare,salvo che il fatto costituisca più grave reato, chiunque commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Esempio: Un dipendente della Società potrebbe accedere al sistema informatico adottato dal tribunale, al fine di alterare o cancellare informazioni raccolte durante un'ipotetica indagine.

Al fine di contrastare la realizzazione di tale fattispecie di reato è previsto apposito presidio di controllo "7.4 Navigazione in internet" che rende nota l'adozione di uno specifico sistema di blocco o filtro automatico per prevenire determinate operazioni quali l'*upload* o l'accesso a determinati siti considerati non pertinenti all'attività operativa

- Danneggiamento di sistemi informatici e telematici (art. 635-quater c.p.);

Oltre ad essere realizzabile mediante le condotte indicate nell'art. 635-bis, è prevista anche la punibilità di chi introduce o trasmette dati, informazioni o programmi. Tale previsione si è resa necessaria per punire specificamente i danneggiamenti realizzabili anche a distanza mediante *malware* introdotti o fatti circolare in rete.

- Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies c.p.);

Si è scelto volutamente di codificare autonomamente tutti quei comportamenti delittuosi commessi ai danni di "Enti pubblici o, ad essi pertinenti, o comunque di pubblica utilità". La semplice "condotta" diretta alla commissione del reato, con eccezione di quanto previsto dall'art. 635-bis, è di per ségià punibile non essendo necessario provare che il comportamento del reo raggiunga lo scopo prefissato, venendo quest'ultimo ad influire solo sulla quantificazione della pena. Il legislatore anticipa la soglia di punibilità al fine di meglio sottolineare e quindi sanzionare tutta una serie di comportamenti illeciti riscontrati in questi anni.

- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);

Secondo il legislatore, l'introduzione di tale fattispecie è indispensabile per coprire alcune condotte tipiche che non rientrerebbero nella frode informatica (640bis).

- **Delitti in materia di strumenti di pagamento diversi dai contanti, introdotti dal D.Lgs. 184/2021 (art. 25 octies I):**

- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater, co. I c.p.).

La norma contempla l'ipotesi in cui, salvo che il fatto costituisca più grave reato, il soggetto che, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

- Frode informatica (640 ter, co. I c.p.).

Il delitto di frode informatica, così come formulato dall'art. 640 ter, co. I c.p., punisce chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. La norma prevede, peraltro, pene diverse a seconda che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale o sia commesso con abuso della qualità di operatore del sistema dall'ipotesi, più grave, in cui il fatto sia commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

- **Reati in materia di violazione del diritto d'autore (art. 25-*novies*).**

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

5. REGOLE GENERALI DI COMPORTAMENTO

Coerentemente con i princìpi deontologici contenuti all'interno del Codice Etico, il personale deve fare riferimento alle seguenti norme comportamentali.

Ogni postazione informatica deve essere gestita nel rispetto della normativa vigente in materia di diritto d'autore, *copyright* e *privacy*, nonché nel rispetto di tutta la normativa nazionale e internazionale concernente l'utilizzo dei mezzi informatici.

Nell'ambito dei processi oggetto del Protocollo, il personale della Società, in particolare, dovrà:

- attuare i comportamenti richiesti dalla Società e necessari per proteggere il sistema informativo, diretti a evitare che terzi possano accedervi in caso di allontanamento dalla postazione di lavoro;
- conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi non autorizzati che in tal modo potrebbero accedere abusivamente a dati aziendali riservati;
- astenersi da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni e dei dati aziendali;
- astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui.

Altresì:

- ogni utente è tenuto a segnalare al proprio responsabile l'eventuale esistenza di *virus* ed eventuali incidenti di sicurezza, mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate, che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- qualora sia previsto il coinvolgimento di soggetti terzi/*outsourcer* nella gestione dei sistemi informatici e del patrimonio informativo nonché nell'interconnessione/utilizzo dei *software* della Pubblica Amministrazione o delle Autorità di Vigilanza, tali soggetti devono impegnarsi a operare nel rispetto della normativa vigente.

In generale, è fatto divieto di:

- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti *software* non autorizzati atti a impedire o interrompere le comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente Pubblico o a essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o dati e programmi a esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui, o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;

- alterare, distrarre o mettere a disposizione d'altri gli strumenti di pagamento diversi dal contante;
- alterare i sistemi informatici al fine di modificare o alterare strumenti di pagamento diversi dal contante.

Le disposizioni del presente Protocollo sono integrate, per quanto qui non espressamente disciplinato e compatibilmente ai predetti principi, dal Regolamento Aziendale per l'utilizzo del Sistema Informatico.

La Società condanna tramite l'applicazione del Sistema Disciplinare i comportamenti difformi ai princìpi sopra menzionati, nonché ai presidi di controllo di seguito riportati.

6. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee <Guida di Confindustria, nonché delle "*best practice*" prevede con riferimento alle aree e alle attività Sensibili individuate:

- *standard di controllo "generali"*, applicabili a tutte le attività sensibili;
- *standard di controllo "specifici"*, applicabili a determinate attività Sensibili e riportati nelle singole Parti Speciali.

I presidi di controllo di carattere generale da considerare e applicare con riferimento a tutte le attività sensibili sono i seguenti:

- *segregazione delle funzioni:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi.
- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase

gestionale e autorizzativa. Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;

- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

Sulla base dei presidi di controllo generali sopra riportati, i presidi di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

a) tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;

b) siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

c) per tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;
- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema di deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

7. PRESIDI DI CONTROLLO SPECIFICI

7.1 GESTIONE DEL PROFILO UTENTE E DEL PROCESSO DI AUTENTICAZIONE

Il sistema informatico è accessibile da ciascun dipendente tramite apposita utenza dedicata. L'accesso al sistema informatico richiede l'inserimento di un *username* e di una *password* individuali e univoci.

È previsto un sistema formale di autorizzazione e registrazione dell'attribuzione, modifica e cancellazione delle utenze, coerente con l'operatività e le responsabilità assegnate.

Sono definite apposite regole per la creazione e gestione delle *password* di accesso (lunghezza minima, regole di complessità, ecc.). Le impostazioni di sistema richiedono l'aggiornamento periodico delle *password* degli utenti almeno ogni sei mesi. È previsto il blocco dell'utenza in caso di un determinato numero di inserimenti consecutivi errati della *password*.

È fatto divieto di utilizzare *password* di altri utenti aziendali, anche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi.

Ogni postazione informatica deve essere dotata di meccanismi di *stand-by* protetti da *password* abbinata a *username* al fine di evitare l'utilizzo della macchina in caso di allontanamento temporaneo dell'utente.

Gli amministratori di sistema sono assegnatari di privilegi speciali autorizzati dal CdA.

7.2 GESTIONE DEI SISTEMI HARDWARE E SOFTWARE

È tenuto e aggiornato un inventario dell'*hardware* e del *software* in uso presso la Società.

Può essere utilizzato solo *software* formalmente autorizzato e certificato. È vietata l'installazione di programmi di qualunque tipo diversi da quelli autorizzati dalla Società.

È fatto divieto di installare nella rete aziendale, o scaricare da Internet, un *software* che non rientri nello scopo per cui il sistema informatico è stato assegnato all'utente e che non sia stato autorizzato dalla Società, per evitare che possa interrompere, danneggiare, manomettere o impedire le comunicazioni informatiche aziendali. È fatto obbligo a ciascun operatore di postazione informatica che necessiti di un apposito programma non già caricato sulla macchina in uso inoltrare la relativa richiesta al Responsabile dei Sistemi Informativi affinché la inoltri all'Ufficio Acquisti che provvederà sulla base della relativa procedura.

È altresì vietato modificare le configurazioni impostate sul proprio *personal computer* e su qualunque altro dispositivo aziendale. Le applicazioni tengono traccia delle modifiche ai dati compiute dagli utenti.

Sono catalogate tutte le macchine presenti evidenziando il *software* caricato, indicando l'eventuale data di scadenza delle singole licenze.

Il Responsabile dei Sistemi Informativi stabilisce verifiche periodiche sui *software* installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di *software* proibiti e/o potenzialmente nocivi.

7.3 USO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. I soggetti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare tale posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali se non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, acquisti *on-line*, concorsi, *forum* o *mailing-list*, se non per ragioni lavorative e solo se espressamente autorizzati dal proprio superiore gerarchico;
- inviare messaggi, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge e a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della nazionalità,

dell'origine etnica, della fede religiosa, dell'età, del sesso, dello stato civile, delle condizioni personali;
- inviare, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico;
- lo svolgimento di azioni non attinenti alle mansioni assegnate.

Tutte le caselle di posta elettronica devono essere oggetto di salvataggio automatico sia per le comunicazioni in ingresso che in uscita.

Sono altresì monitorati i volumi di trasferimento di messaggi di posta elettronica o di file che per dimensioni o caratteristiche potrebbero contenere opere dell'ingegno protette. La documentazione elettronica che costituisce per l'azienda *knowhow* aziendale tecnico o commerciale protetto e che, quindi, viene contraddistinta da diciture o avvertenze dirette a evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione dell'Amministratore Delegato.

Successivamente alla cessazione del rapporto di lavoro, la Società può liberamente accedere ai dispositivi aziendali concessi in dotazione all'utente nonché alla casella di posta elettronica assegnata al lavoratore durante il rapporto di lavoro per ragioni di continuità dell'attività della Società o per finalità di sicurezza del sistema informatico.

7.4 NAVIGAZIONE IN INTERNET

Il dispositivo abilitato alla navigazione in *Internet* costituisce strumento aziendale necessario allo svolgimento dell'attività lavorativa assegnata. È, quindi, assolutamente proibita la navigazione in *Internet* per motivi diversi da quelli strettamente legati all'attività lavorativa.

All'utente non è consentito:

- accedere a siti *Internet* evitando o superando - o comunque tentando di superare o disabilitando - i sistemi adottati dalla Società per bloccare l'accesso ad alcuni siti e in ogni caso utilizzare siti o altri strumenti (es. *cracking programs*) che realizzino tale fine;
- accedere a siti *Internet* che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, delle condizioni personali.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, Rangers S.r.l. rende nota l'adozione di uno specifico sistema di blocco o filtro automatico per prevenire determinate operazioni quali l'*upload* o l'accesso a determinati siti considerati non pertinenti all'attività operativa o che presentino contenuti illeciti (siti di pedopornografia, che promuovono movimenti terroristici o sovversivi, che effettuano attività di pirateria informatica, ecc.).

Il servizio di connessione *Internet* aziendale, altresì, non deve essere utilizzato per commettere azioni punibili o reprensibili quali, per esempio, infrangere i diritti di proprietà intellettuale e visitare siti pornografici.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare *Internet* per:

- l'*upload* o il *download* di *software* gratuiti (*freeware*) e *shareware*, nonché l'utilizzo di documenti - anche filmati e musica - se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione da parte del personale dell'Ufficio Sistemi Informativi;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, fatti salvi i casi direttamente autorizzati dal proprio superiore gerarchico e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a *forum* non professionali, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in *guest book* anche utilizzando pseudonimi (o *nickname*) se non espressamente autorizzati dal proprio superiore gerarchico;
- l'accesso, tramite *Internet*, a caselle *webmail* di posta elettronica personale.

È garantito, laddove possibile, il monitoraggio dell'utilizzo di *Internet* da parte del personale su qualunque dispositivo aziendale (*computer* fissi, *computer* portatili, *tablet*, *smartphone)*, compatibilmente con le vigenti disposizioni in materia di tutela della riservatezza dei lavoratori, compresa l'immissione o acquisizione di contenuti mediante utilizzo della rete aziendale o esterna.

Gli eventuali controlli, compiuti dal personale incaricato della gestione dei sistemi informativi, potranno avvenire mediante un sistema di controllo dei contenuti (*proxy server*) o mediante "*file di log*" della navigazione svolta.

Il controllo sui *file di log* non è continuativo e i *file* stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

I *file* privati scaricati sul dispositivo aziendale dall'utente non saranno oggetto di cancellazione da parte del personale incaricato della gestione dei sistemi informativi, qualora possano essere eventualmente presentati come prova in un eventuale contenzioso giudiziario.

7.5 GESTIONE DEI DOCUMENTI INFORMATICI PUBBLICI O PRIVATI AVENTI EFFICACIA PROBATORIA

In caso di utilizzazione di documenti informatici integranti atto pubblico, certificato, autorizzazione amministrativa, copia autentica, attestato, scrittura privata, è fatto obbligo di verificare la provenienza e la veridicità del documento e del suo contenuto e di conservare il documento cartaceo e la relativa documentazione cartacea probante la veridicità del suo contenuto.

Qualora la provenienza e/o la veridicità del documento o del suo contenuto siano dubbi, è fatto obbligo di bloccare il procedimento di predisposizione e informare senza indugio il Responsabile della Funzione coinvolta e l'Organismo di Vigilanza.

Sono assolutamente vietate le pratiche finalizzate a comunicare informazioni false, errate o comunque manipolate, anche in forma elettronica, mediante l'alterazione di dati o programmi informatici, allo scopo di inficiare il processo decisorio e/o di valutazione della Pubblica Amministrazione, procurando così vantaggi non dovuti alla Società e danni ingiusti allo Stato, agli altri enti pubblici, all'Unione europea.

L'utilizzo di sistemi informativi aziendali per espletare gli adempimenti verso gli Enti della Pubblica Amministrazione, che prevedano il ricorso a *software* forniti dagli enti pubblici ovvero la connessione

diretta con gli stessi, deve avvenire assicurando protocolli di sicurezza fisica e di sicurezza informatica, secondo gli *standard* e le *best practice* in uso sul mercato e nel sistema.

7.6 SICUREZZA DEI SISTEMI INFORMATIVI

Tutti gli strumenti informatici sono dotati di *software anti-virus* al fine di effettuare un controllo *anti-virus* anche su *media* esterni. Ogni utente è tenuto a segnalare al proprio responsabile l'eventuale esistenza di *virus* ed eventuali incidenti di sicurezza, mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente. È severamente vietato disinstallare i programmi di protezione installati.

Non è consentito collegare alla rete aziendale nessun apparato che non sia stato codificato, configurato e approvato dall'Ufficio Sistemi Informativi. Non è consentito l'utilizzo di chiavette USB, CD-ROM, DVD di provenienza ignota e personale.

Tutti i *file* di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e alla relativa autorizzazione all'utilizzo da parte degli amministratori del sistema.

Se necessario, Rangers S.r.l. può effettuare ai sensi di legge dei controlli mirati al fine di verificare il corretto utilizzo degli strumenti di lavoro. In particolare, il personale incaricato potrà eseguire controlli sui documenti presenti nei *device* aziendali qualora sussista la necessità di:

a) proseguire con l'attività aziendale in assenza del dipendente interessato;

b) rilevare le cause di eventuali anomalie dei sistemi, presenza di *virus* informatici, esecuzione di manutenzioni, *back-up*;

c) verificare possibili cause di abuso nell'utilizzo degli strumenti elettronici.

La Società adotta specifiche misure di protezione a mitigazione dei rischi connessi all'utilizzo di I*nternet* quali, per esempio, sistemi di *firewall* a protezione dagli accessi non autorizzati.

Il Responsabile dei Sistemi Informativi individua le persone fisiche abilitate all'accesso al *server* aziendale, ai sistemi informatici e alle banche dati, e autorizza l'attività che deve essere svolta. È vietata esplicitamente ogni attività estranea all'operatività aziendale.

Ogni anomalia che dovesse essere riscontrata nel corso dell'accesso a un sistema informatico o telematico altrui deve essere segnalata al Responsabile dei Sistemi Informativi che, qualora lo ritenga opportuno, informa l'Organismo di Vigilanza.

7.7 INSTALLAZIONE E GESTIONE DI SISTEMI DI VIDEOSORVEGLIANZA

È responsabilità della Divisione Vigilanza adottare adeguate misure affinché sia assicurato che le apparecchiature di videosorveglianza installate presso le sedi e i locali dei clienti siano conformi alle specifiche norme contrattuali e in ogni caso il loro utilizzo sia tale da garantire di non incorrere nella commissione dei reati di cui all'art. 24-*bis* del D.lgs. 231/2001 e in particolare, ai reati di:

- accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*c.p.);

- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.).

In particolare, il Direttore Divisione Vigilanza si coordinerà con il DPO per fare in modo che le apparecchiature installate non siano utilizzate dagli operatori come strumento di divulgazione di immagini o comunicazioni e affinché, in generale, siano rispettate le disposizioni in materia di protezione dei dati.

Qualora l'installazione di apparecchiature di videosorveglianza presso le sedi e i locali dei clienti fosse affidata a fornitori esterni, questi dovranno essere opportunamente qualificati così come previsto dalla relativa procedura adottata in Azienda.

7.8 SOFTWARE ANTIRICICLAGGIO

Sono definiti all'interno del Manuale Antiriciclaggio adottato dalla Società, cui si rinvia, gli obblighi di registrazione e di conservazione dei documenti e delle informazioni richiesti dal D.lgs. 231/2007, come integrato dal D.lgs. 90/2017, in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. Tali informazioni sono adeguatamente archiviate in appositi sistemi informativi aziendali, affinché possano essere utilizzate per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dalla UIF o da qualsiasi altra Autorità competente.

La Società, al fine di adempiere compiutamente alle prescrizioni imposte dalla normativa di riferimento, utilizza un apposito *software* antiriciclaggio, creato al fine di raccogliere, conservare e analizzare i dati raccolti e rilevare, per poi segnalare alle autorità competenti, eventuali operazioni sospette.

7.9 PROCEDURA DI WHISTLEBLOWING

Nel rispetto delle disposizioni di legge per la tutela del dipendente che segnala reati o irregolarità di cui sia venuto a conoscenza nell'ambito del rapporto di lavoro, Rangers S.r.l. si dota di appositi canali attraverso i quali effettuare la segnalazione di violazioni, che siano idonei a garantire la riservatezza dell'identità del segnalante e degli altri soggetti coinvolti nella segnalazione. La Società assicura, altresì, la tutela dei soggetti coinvolti da possibili atti ritorsivi, diretti o indiretti, ricollegabili alla segnalazione.

Nello specifico, la Società di è dotata di un canale informatico di segnalazione nonché di una specifica policy whistleblowing volta a disciplinare le tipologie di violazione oggetto di segnalazione e la procedura in uso, cui si rinvia per i dettagli operativi. La segnalazione può esser effettuata mediante accesso al seguente link: https://rangerswhistleblowing.battistolli.it/). Attraverso tale strumento, nel rispetto della *privacy* e dei diritti individuali, tutti coloro i quali vengono a conoscenza di eventuali casi di illeciti rilevanti per il D.lgs. 231/2001, violazioni del Modello e del Codice Etico nonché violazioni ai sensi del D.lgs. n. 231/2007 e degli altri sistemi di compliance adottati, possono segnalare liberamente le violazioni riscontrate, in maniera riservata. L'Ufficio Segnalazioni Illeciti Whistleblowing provvederà alla gestione della segnalazione, nel rispetto del principio di riservatezza del segnalante e degli altri soggetti coinvolti.

Per la individuazione precipua della procedura di segnalazione, della processione della segnalazione e della tutela del segnalante, ci si riporta alla Parte Generale del presente MOG adottato dalla Società.

8. LA TUTELA DEI DATI PERSONALI

L'entrata in vigore del GDPR ha ampliato la definizione di dato personale e sensibile, che non si riferiscono più unicamente ai a dati quali indirizzo o numero di telefono, ma comprendo anche dati identificativi *online* come *cookie*, indirizzi IP, geolocalizzazione ed *email*.

Il Regolamento, infatti, individua quattro macro-categorie di interesse:

- dati personali: informazioni che identificano la persona, incluso nome, cognome, caratteristiche fisiche, identificativi online;
- dati genetici: dati ottenuti tramite analisi di DNA o RNA da un campione biologico;
- dati biometrici: caratteristiche fisiche identificative della persona, come l'impronta digitale, l'iride o l'immagine facciale;
- dati sulla salute: qualsiasi dato relativo alla salute, fisica o mentale.

Per adeguarsi al nuovo regolamento, nel raccogliere i dati, le aziende devono seguire le seguenti regole:

- permettere all'utente di fornire il proprio consenso in modo esplicito e tracciabile;
- predisporre un'informativa sul trattamento dei dati personali trasparente, chiara e facilmente accessibile;
- garantire che i dati raccolti siano pertinenti, adeguati e limitati alle finalità per cui vengono richiesti e trattati.

La richiesta di consenso deve essere chiara, comprensibile e deve essere presentata in una schermata facilmente riconoscibile. Bisogna, inoltre, garantire all'utente il diritto di revocare il proprio consenso in qualsiasi momento.

Emerge dunque una maggiore responsabilizzazione per le aziende, dovendo garantire la massima sicurezza dalla fase di raccolta sino a quella di elaborazione e conservazione dei dati.

Nel regolamento viene introdotto il diritto alla "portabilità" dei propri dati personali, pertanto viene concessa la possibilità a qualsiasi utente di trasferire i dati da un titolare del trattamento a un altro. Il cittadino, cioè, deve poter ottenere facilmente una copia dei propri dati personali, in un formato leggibile e facilmente trasferibile.

La norma trova un'eccezione nei casi i cui si tratta di dati contenuti in archivi pubblici, come ad esempio l'ufficio anagrafe; in questo caso il diritto non potrà essere esercitato.

Sono stati poi ampliati gli obblighi sussistenti in capo al Titolare e al Responsabile del trattamento (artt. 24 e ss..).

Essi non dovranno solo garantire il rispetto delle regole fissate per il trattamento dei dati personali, ma dovranno adottare una serie di misure giuridiche, organizzative e tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, adeguati al settore di interesse in cui svolge la propria attività.

Eventuali violazioni di dati personali vanno comunicate all'Autorità Garante da parte del Titolare del trattamento; il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Tra i principali obblighi cui le aziende devono attenersi vi è l'adozione del Registro dei trattamenti di dati personali (art. 30).

Il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare i danni; potrà decidere di non informarli qualora ritenga che la violazione non comporti un rischio elevato per i loro diritti o se dimostrerà di avere già adottato misure di sicurezza o ancora nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato al rischio.

L'Autorità Garante potrà imporre al titolare del trattamento di informare gli interessati, sulla base di una propria valutazione dei rischi correlati alla violazione commessa.

Tra i principali obblighi previsti dal nuovo regolamento europeo sulla privacy c'è quello, per alcune società, di adeguare il proprio organigramma privacy inserendo all'interno dello stesso la figura del DPO, Data Protection Officer (art. 37).

Il Responsabile della protezione dei dati personali, incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti ha il compito principale del DPO di osservare, valutare e gestire i dati personali allo scopo di far rispettare le normative europee e nazionali in materia di privacy.

Il DPO è una figura professionale, con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi e dotato di conoscenze specialistiche della normativa e delle prassi in materia di protezione dati, nonché delle norme e delle procedure amministrative che caratterizzano il settore in cui opera.

Importante è garantire l'autonomia decisionale e l'estraneità del DPO rispetto alla determinazione delle finalità e delle modalità del trattamento dei dati; è tenuto in ogni caso al segreto e alla riservatezza in ordine alle sue funzioni di responsabile della protezione.

A seguito del recepimento del Regolamento UE sulla privacy, la società ha adottato una nuova procedura in linea con quanto prescritto dalla normativa, per il cui contenuto si rinvia al documento adottato.

9. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Al fine di verificare il rispetto delle procedure relative al processo in oggetto, il Responsabile Sistemi Informativi invia all'Organismo di Vigilanza, con periodicità definita dallo stesso, apposite relazioni inerenti allo sviluppo e all'aggiornamento dei sistemi informativi aziendali, segnalando eventuali ipotesi di anomalie verificatesi ma non oggetto di immediata segnalazione.

Inoltre, i Responsabili degli Uffici aziendali o chiunque rilevi anomalie nell'utilizzo dei sistemi informatici e telematici della Società è tenuto a informare tempestivamente l'Organismo di Vigilanza sulle criticità di sistema riscontrate.

Conformemente a quanto stabilito nella Parte Generale del Modello 231, fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli di propria iniziativa o a seguito delle segnalazioni ricevute, esso effettua periodicamente controlli a campione sulle attività di "Gestione delle infrastrutture tecnologiche e dei sistemi informativi", diretti a verificare il rispetto delle procedure indicate.

10. CONSERVAZIONE DELLA DOCUMENTAZIONE

Tutta la documentazione (elettronica e cartacea) prodotta nell'ambito delle attività inerenti il funzionamento dei sistemi informativi aziendali, è conservata a cura del Responsabile Sistemi Informativi e messa a disposizione su richiesta del Presidente del CdA, del Consiglio di Amministrazione e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

PARTE SPECIALE VIII

PROTOCOLLO DI CONFORMITÀ AL D.LGS. 231/2001 RELATIVO AL PROCESSO

GESTIONE DELLE OPERAZIONIE DEGLI ADEMPIMENTI FISCALI

INDICE

1. FINALITÀ 2

2. IL SISTEMA DEI CONTROLLI 2

2.1. STANDARD DI CONTROLLO GENERALI 2
2.2. STANDARD DI CONTROLLO SPECIFICI 3

3. AMBITO DI APPLICAZIONE 5

3.1 LE ATTIVITÀ A POTENZIALE "RISCHIO REATO" 5
3.2 LE FUNZIONI AZIENDALI COINVOLTE 5

4. NORMATIVA DI RIFERIMENTO 5

5. REATI ASTRATTAMENTE PERPETRABILI 6

6. REGOLE GENERALI DI COMPORTAMENTO 9

7. PRESIDI DI CONTROLLO 11

7.1 SELEZIONE DEL CONTRAENTE 11
7.2 STIPULA E VERIFICA DEI CONTRATTI/FORNITURA 12
7.3 SISTEMA E INFRASTRUTTURE IT 13

8. CONSERVAZIONE DELLA DOCUMENTAZIONE 14

9. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA 14

1. FINALITÀ

Il presente Protocollo regola le attività operative e i controlli-chiave tendenti alla prevenzione dei reati indicati nel D.lgs. 231/2001. L'obiettivo è quello di definire ruoli, responsabilità, modalità operative e codici comportamentali cui tutto il Personale deve attenersi nell'ambito del processo di "**Gestione delle operazioni e degli adempimenti fiscali**".
Il Protocollo è redatto in conformità alle norme comportamentali richiamate nel Codice etico, nella parte generale del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società, nelle procedure e istruzioni operative, e nelle disposizioni interne aziendali.
Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- Indicare le procedure che i membri degli Organi Sociali, le Funzioni Aziendali, i Dipendenti, i Collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello;

- Fornire all'OdV e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei Dipendenti – in via diretta – dei Collaboratori Esterni – limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e codici comportamentali e nelle specifiche clausole inserite nei contratti in attuazione - di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da - considerati individualmente o collettivamente - integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

2. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria e dal Decreto n. 125/2019 e successivo Provvedimento del Direttore dell'Agenzia delle Entrate di aprile 2016 nonché delle "*best practice*", prevede con riferimento alle Aree e alle Attività Sensibili individuate:

- *livelli di controllo "generali"*, applicabili a tutte le Attività Sensibili;
- *livelli di controllo "specifici"*, applicabili a determinate Attività Sensibili e riportati nelle singole Parti Speciali.

2.1. STANDARD DI CONTROLLO GENERALI

Gli standard di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili sono i seguenti:

- *segregazione delle funzioni/attività:* si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla; è previsto che nello svolgimento di qualsiasi attività, siano coinvolti in fase attuativa, gestionale e autorizzativa soggetti diversi dotati delle adeguate competenze. Tale presidio è funzionale nel suo complesso a mitigare la discrezionalità gestionale nelle attività e nei singoli processi;
- *norme/circolari:* devono esistere all'interno dell'azienda disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- *poteri autorizzativi e di firma*: i poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all'interno della società;
- *tracciabilità*: ogni operazione relativa all'attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex *post*, anche tramite appositi supporti documentali. Tale regola prevede che nello svolgimento delle attività, vengano adottate le cautele necessarie a garantire l'efficace ricostruibilità nel tempo degli aspetti sostanziali del percorso decisionale e di controllo che ha ispirato la successiva fase gestionale e autorizzativa- Tale presidio è funzionale a garantire la trasparenza delle attività e la ricostruibilità della correttezza gestionale di ciascun processo;
- *compliance*: nell'esecuzione del processo in oggetto tutti i dirigenti, dipendenti, collaboratori nonché soggetti esterni devono operare conformemente al Modello e al Codice Etico.

2.2. STANDARD DI CONTROLLO SPECIFICI

Sulla base degli standard di controllo generali sopra riportati, gli standard di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

- tutte le operazioni, la formazione e l'attuazione delle decisioni della Società rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure aziendali;
- siano definite e adeguatamente comunicate le disposizioni aziendali idonee a fornire regole di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- per tutte le operazioni:

    - siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno dell'azienda, nonché i livelli di dipendenza gerarchica e la descrizione delle relative responsabilità;
    - siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;

- la Società adotti strumenti di comunicazione dei poteri di firma conferiti e un sistema delle deleghe e procure;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche.

Il seguente Protocollo, sviluppato al fine di minimizzare il rischio di operare in violazione di norme tributarie, ovvero in contrasto con i principi o le finalità dell'ordinamento, è articolato sui seguenti elementi cardine:

❖ **Ruoli e responsabilità**

Il sistema di gestione del rischio fiscale prevede due diverse linee di controllo:

- il controllo di primo livello, o "controllo di linea", il quale è direttamente messo in atto dalla Direzione Amministrazione, Finanza e Controllo Corporate relativamente agli adempimenti tributari e fiscali ordinari;
- il controllo di secondo livello, che è esercitato dagli organi preposti (sindaco unico, i revisori, l'Organismo di Vigilanza etc.) che ha l'obiettivo di valutare la funzionalità complessiva del sistema, nonché determinare eventuali andamenti anomali o violazioni della procedura.

Dal punto di vista operativo, la separazione dei compiti non deve, tuttavia, produrre una netta separazione tra le funzioni di *business* e la funzione fiscale; al contrario, si ritiene necessario che questa sia coinvolta in modo costante e totale a monte delle decisioni di *business*. Tale coinvolgimento è garantito quando il responsabile fiscale contribuisce attivamente alle decisioni di operazioni o progetti fondamentali per la società.

❖ **Flussi informativi e *reporting***

Al fine di garantire una veloce e aggiornata circolazione delle informazioni al proprio interno, l'impresa deve predisporre opportuni flussi informativi.
Un ruolo rilevante e centrale è svolto dal Sindaco Unico, specie in riferimento a tutte quelle operazioni societarie che hanno riflessi su aspetti sia contabili che fiscali in quanto, ai sensi dell'art. 2403 c.c. e come confermato dalla giurisprudenza ormai consolidata, il Sindaco Unico è tenuto a vigilare sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento, oltreché a svolgere il controllo contabile nei casi previsti.
Altro ruolo determinate è svolto dall'Organismo di Vigilanza, sia in termini di verifiche dirette e indirette per il tramite di altre funzioni e organi, su tematiche fiscali, sia quale soggetto responsabile del coordinamento di tali verifiche e controlli.

Gestire il rischio fiscale significa, anzitutto, presidiarlo. Da qui la necessità di realizzare anche una

reportistica in chiave preventiva del rischio fiscale che permetta, a sua volta, un monitoraggio costante dei rischi aziendali, fornendo al *management* un'informativa completa, aggiornata e tempestiva.

3. AMBITO DI APPLICAZIONE

Il presente Protocollo si applica a Rangers S.r.l. (di seguito anche denominata "la Società"), in conformità alle prescrizioni del D.lgs. 231/2001 ed è rivolto a tutti i soggetti aziendali coinvolti, a vario titolo, nel processo di Gestione delle operazioni e degli adempimenti fiscali.

3.1 LE ATTIVITÀ A POTENZIALE "RISCHIO REATO"

Concerne, in particolare, tutte quelle funzioni/uffici interessati e coinvolti nei seguenti processi:

- Ricerca e selezione dei fornitori/consulenti;
- gestione del processo di qualifica e valutazione del fornitore/consulente;
- gestione ed emissione degli ordini di acquisto/contratti;
- formalizzazione dei rapporti con i consulenti/fornitori di servizi;
- verifica e monitoraggio delle prestazioni rispetto al contratto/ordine;
- monitoraggio delle merci/servizi ricevuti in conformità con l'ordine di acquisto/contratto;
- rilevazione ed elaborazione delle informazioni contabili necessarie alla corretta e completa compilazione delle fatture;
- conservazione dei documenti contabili.

3.2 LE FUNZIONI AZIENDALI COINVOLTE

Le Funzioni aziendali coinvolte a qualsiasi titolo nella presente procedura sono:

- Ufficio Acquisti Corporate;
- Direzione Amministrazione, Finanza e Controllo Corporate;
- Ufficio Affari Legali Corporate;
- Direzione Risorse Umane Corporate;
- Direzione Commerciale;
- Responsabile Controllo e Recupero Crediti;
- Responsabile Ufficio Contratti;
- Soggetto richiedente la prestazione/servizio.

4. NORMATIVA DI RIFERIMENTO

Al fine di garantire il rispetto delle procedure aziendali, i soggetti a vario titolo coinvolti nelle diverse fasi del presente processo hanno l'obbligo di osservare la seguente normativa di riferimento:

- D.lgs. 8 giugno 2001 n. 231 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 30*";
- L. 19 dicembre 2019, n. 157, conversione con modificazioni, del d.l. 26 ottobre 2019, n.124 recante "*disposizioni urgenti in materia fiscale e per esigenze indifferibili*".

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello 231 di Rangers S.r.l.;
- Protocollo sulla "Gestione dei rapporti con la Pubblica Amministrazione e delle liberalità";
- Protocollo sulla "Gestione degli approvvigionamenti";
- Protocollo sulla "Gestione della Tesoreria";
- Codice Etico del Gruppo Battistolli;
- Procedure e istruzioni operative;
- Istruzioni Operative Ufficio Contratti;
- Linee-guida e regolamenti;
- Procure, deleghe e disposizioni organizzative;
- Manuale della Qualità;
- Manuale di gestione del *software* di contabilità in uso;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione.

5. REATI ASTRATTAMENTE PERPETRABILI

Di seguito sono individuate specifiche procedure volte a prevenire il compimento dei reati presupposto, di cui al D.lgs. 231/01, come elencati:

- **Reati tributari, introdotti dalla L. n. 157/2019 (art. 25-*quinquiesdecies*):**

  - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. n. 74/2000)

L'art. 2 del D.lgs 74/2000 prevede che sia punito chiunque al fine di evadere le imposte sui redditi e l'Iva indica in una dichiarazione elementi passivi fittizi attraverso fatture o altri documenti per operazioni inesistenti. Secondoconsolidata giurisprudenza, integra il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, la falsa indicazione, nella dichiarazione Irpef, di spese deducibili dall'imposta, quando le stesse non siano state effettuate o siano state effettuate in misura inferiore. (cfr.Cass. civ., n. 48486/2011 e 27392/2012). In relazione al mezzo fraudolento di cui l'agente si avvale per l'indicazione in dichiarazione di elementi passivi fittizi, la Corte di cassazione ha fornito, una definizione degli altri documenti rilevanti ai sensi dell'art. 2 del d.lgs. n. 74/2000, precisando che tali sono quelli «[…] aventi, ai fini fiscali, valore probatorio analogo alle fatture (documenti tipici fiscali previsti espressamente dal d.P.R. 633/1972, art. 21)». Pertanto, può dirsi che ai fini della sussistenza del reato di dichiarazione fraudolenta di cui all'art. 2 del d.lgs. 74/2000, per fatture o altri documenti per operazioni inesistenti devono intendersi quelli che, a prescindere dal *nomen*, hanno l'attitudine, in base alle norme dell'ordinamento tributario, a fornire la prova delle operazioni in essi documentati. A tal fine non è necessario stabilire *ex post* se il documento possa avere tale attitudine ma è sufficiente che, per le sue caratteristiche estrinseche e per il suo contenuto, tale natura non possa essere esclusa *ictu oculi* in base alle norme dell'ordinamento tributario sin dalla fase dell'accertamento fiscale (Cassazione penale sez. III, 27/02/2018, n.40448).

Esempio: Il personale della società, nell'ambito dell'attività di gestione di acquisti di beni/servizi, stipula contratti di acquisto di beni o servizi inesistenti, al solo fine di poter registrare elementi passivi fittizi ed evadere le imposte sui redditi; oppure, il personale della società, nell'ambito dell'attività emissione e contabilizzazione di fatture/note di credito, contabilizza fatture per operazioni inesistenti al fine di registrare elementi passivi fittizi ed evadere le imposte sui redditi.

  - Dichiarazione fraudolenta mediante altri artifici (art.3 D.lgs n. 74/2000)

La dichiarazione fraudolenta potrà essere realizzata, oltre che con le modalità previste dall'articolo precedente, anche con l'utilizzo di altri artifizi. Quest'ultima è costruita, essenzialmente, come frode contabile, alla quale deve associarsi un *quid pluris* artificioso non tipizzato (diverso dall'uso di fatture o altri documenti falsi, integrante l'ipotesi di cui al precedente art. 2) ma, comunque, caratterizzato dall'idoneità a indurre in errore e a impedire il corretto accertamento della realtà contabile del soggetto che presenta la dichiarazione annuale d'imposta, come:la tenuta di un sistema parallelo di contabilità "nera"; la vendita "a nero" organizzata in locali contigui a quelli aziendali; la voluta "confusione" di ricavi provenienti da fonti diverse in modo da impedire di individuare il titolare degli stessi; lo spostamento artificioso di redditi tra soggetti rivolto a fare figurare come percepiti da terzi redditi propri del contribuente.

Esempio: Il personale della società, nell'ambito dell'attività di ricerca, selezione e qualifica dei fornitori, omettendo attività di verifica sull'esistenza e l'operatività del fornitore, qualifica controparti fittizie (cd. Società "cartiere" che si interpongono tra l'acquirente e l'effettivo cedente del bene), con le quali saranno contabilizzate operazioni "soggettivamente" inesistenti.

- Dichiarazione infedele (art. 4 D. Lgs. n. 74/2000)

Fuori dei casi previsti dagli articoli 2 e 3, è punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni. La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).

- Omessa dichiarazione (art. 5 D.lgs. n. 74/2000)

È punito chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila. La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).

- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs n. 74/2000)

L'art. 8 del D.lgs n. 74/2000 punisce chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.La realizzazione della condotta *de qua* necessita che la fattura o il documento escano dalla sfera di fatto e di diritto dell'emittente mediante consegna o spedizione a un terzo potenziale utilizzatore, che non abbia partecipato alla perpetrazione del falso. La condotta delittuosa in esame, si pone all'inizio di un percorso che porterà, nella maggior parte dei casi, all'utilizzo di tali documenti e quindi al concretizzarsi del reato di cui all'art. 2 – dichiarazione fraudolenta - realizzando appieno quel *fine di consentire a terzi l'evasione*. Sono reati legati dall'unicità del fine, nel senso che il primo (art. 8) costituisce il mezzo normale per realizzare il secondo (art. 2).

- Occultamento o distruzione di documenti contabili (art. 10 D.lgs n. 74/2000)

L'art. 10 del D.lgs n. 74/2000 prevede la reclusione per chiunque, al fine di evadere le imposte sui redditi e l'Iva, ovvero consentire l'evasione a terzi, occulta o distrugge le scritture contabili o i documenti di cui è obbligatoria la conservazione. Secondo la giurisprudenza, ai fini della configurazione del reato, non è sufficiente un mero comportamento omissivo, ossia la omessa tenuta delle scritture contabili, che renda obiettivamente più difficoltosa -ma non impossibile- la ricostruzione della situazione contabile ma è necessario un "quid pluris" a contenuto commissivo consistente nell'occultamento o nella distruzione dei documenti contabili la cui istituzione e tenuta è obbligatoria per legge (Cass. Pen., Sez. 3, n. 19106 del 02/03/2016).

Esempio: Il personale della società, nella tenuta e custodia della documentazione obbligatoria e delle scritture contabili, ambito dell'attività di ricerca, selezione e qualifica dei fornitori, occulta o distrugge scritture contabili o documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi ed evadere le imposte.

- Indebita compensazione (art. 10 *quater* D. Lgs. n. 74/2000)

È punito chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro. È punito chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro. La condotta è rilevante ai fini 231 quando presenta elementi di transnazionalità e rilevanza (imposta IVA evasa >10 mln/€).

- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.lgs n. 74/2000)

Nella nozione di atti fraudolenti, rilevante ai fini della configurabilità del delitto di sottrazione fraudolenta al pagamento delle imposte, rientrano tutti quei comportamenti che, anche se formalmente leciti, risultino connotati da elementi di inganno o di artificio dovendosi ravvisare l'esistenza di uno stratagemma tendente a sottrarre le garanzie patrimoniali all'esecuzione. Tale reato si configura, sotto il profilo oggettivo, sia mediante una vendita simulata sia attraverso il compimento di altri atti fraudolenti. Secondo la previsione normativa questi ultimi debbono essere «idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva». E ciò anche in aderenza all'interesse protetto dalla norma a rendere possibile la riscossione nei confronti del contribuente (bene giuridico peraltro protetto a livello costituzionale dall'art. 53 Cost.). La Suprema Corte, ha affermato, in materia di sottrazione fraudolenta, che: la natura : «la natura fraudolenta degli atti dispositivi presuppone non soltanto la lesione di un diritto altrui, per effetto della riduzione del patrimonio del debitore che rende più difficoltosa l'azione di recupero dell'erario, ma anche che il pregiudizio arrecato non sia immediatamente percepibile»(Cass. pen., Sez. III, 16 maggio 2017,n. 10161). Deve, invece, rilevarsi come per vendita simulata debba intendersi una «alienazione finalizzata a creare una situazione giuridica apparentemente diversa da quella reale, sicché l'alienazione è simulata quando il programma contrattuale non corrisponde deliberatamente in tutto (simulazione assoluta) o in parte (simulazione relativa) alla effettiva volontà dei contraenti» (Cass. pen., Sez. III, 5 luglio 2016, n. 3011); ancora, il negozio può essere simulato sotto il profilo "oggettivo" o "soggettivo" a seconda che gli artifici riguardino gli elementi afferenti il bene compravenduto ovvero le parti che vi sono coinvolte (*ex plurimis*Cass.pen., Sez. III, 06 marzo 2008, n. 14720).

- **Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, introdotti dal D.Lgs. 184/2021 e modificati dalla L. n. 137/2023 (art. 25 octies I):**

  - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter, co. I c.p.).

Il delitto di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, così come formulato dall'art. 493 ter, co. I c.p., punisce chi indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti. La norma contempla, altresì, l'ipotesi del soggetto che falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. La novella del legislatore estende il campo della condotta, contemplando ogni strumento di pagamento diverso dal contante che sia idoneo ad abilitare al prelievo del denaro o all'acquisto di beni o prestazione di servizi o comunque rappresenti uno strumento di pagamento diverso dal contante.

- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater, co. I c.p.).

La norma contempla l'ipotesi in cui, salvo che il fatto costituisca più grave reato, il soggetto che, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

- Frode informatica (640 ter, co. I c.p.).

Il delitto di frode informatica, così come formulato dall'art. 640 ter, co. I c.p., punisce chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. La norma prevede, peraltro, pene diverse a seconda che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale o sia commesso con abuso della qualità di operatore del sistema dall'ipotesi, più grave, in cui il fatto sia commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

- Trasferimento fraudolento di valori (art. 512 *bis* c.p.)

Tale fattispecie punisce, salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648 bis, e 648 ter. Con l'inserimento della presente norma il legislatore ha inteso sanzionare penalmente la condotta fraudolenta di chi trasferisca fittiziamente ad altri denaro od altri beni al fine di elidere l'applicazione delle disposizioni in materia di mezzi di prevenzione patrimoniale, contrabbando ovvero al fine di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio. Tale fattispecie è volta a coprire la condotta di chi non trasferisca effettivamente la titolarità dei beni o del denaro, ma lo faccia fittiziamente, continuando dunque ad avere la disponibilità materiale degli stessi e continuando dunque a goderne.

Le fattispecie di reato sopra indicate sono riportate nella tabella dei reati presupposto aggiornata allegata al Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001 della Società.

6. REGOLE GENERALI DI COMPORTAMENTO

Coerentemente con i princìpi deontologici aziendali di cui al Codice Etico del Gruppo Battistolli, il personale della Società deve far riferimento alle seguenti regole di comportamento:

- lealtà, correttezza, trasparenza, competenza, professionalità, criteri di concorrenza ed economicità nella scelta dei fornitori/professionisti e nella gestione dei rapporti con gli stessi;
- principio di equità nell'erogazione di tutti i compensi e/o somme corrisposte per forniture/incarichi professionali, sulla base di valutazioni obiettive e imparziali, nonché l'adeguata tracciabilità della documentazione relativa alle offerte;
- imparzialità nella selezione dei fornitori/professionisti e nella determinazione delle condizioni d'acquisto di beni e servizi, affinché avvengano sulla base di valutazioni obiettive, fondate sulla qualità, sul prezzo e sulle garanzie fornite;
- nella gestione delle attività contabili devono essere osservate scrupolosamente le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla legge e dai principi contabili nazionali o internazionali applicabili, in modo tale che ogni operazione sia, oltre che correttamente registrata anche autorizzata, verificabile, legittima, coerente e congrua;
- ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto ed essere effettuata in conformità e coerenza con le Istruzioni Operative utilizzando esclusivamente il *software* dedicato. Pertanto, sarà compito della Direzione Amministrazione, Finanza e Controllo per le attività a questa attribuite nell'ambito dell'organigramma aziendale assicurare che la documentazione di supporto sia facilmente reperibile e ordinata secondo criteri logici oltre che immediatamente disponibile per ogni eventuale attività di *audit* interno.
- i dati vengono, altresì, sempre assunti esclusivamente tramite sistemi informatici in grado di verificare, per il ciclo passivo di fatturazione, la corrispondenza tra l'impegno di spesa assunto e il relativo impiego di risorse; per il ciclo attivo, la piena corrispondenza tra le effettive prestazioni erogate, il valore delle stesse e le richieste in pagamento rivolte ai soggetti pubblici/privati. L'intero processo di acquisizione dei dati relativi alle poste contabili attive e passive viene realizzato dalla Società per il tramite di apposito *software*;
- il personale amministrativo della Società, rappresentando una componente significativa del rischio fiscale, deve essere adeguatamente formato sulla normativa in materia, anche in considerazione del continuo e rapido evolversi della normativa stessa. Ulteriore aspetto della formazione del personale amministrativo dovrà riguardare l'utilizzo dei sistemi informatici volti a prevenire qualsiasi manipolazione non autorizzata e garantire un sufficiente livello di protezione dei dati.

Coerentemente è fatto divieto di:

- effettuare prestazioni o pagamenti in favore di collaboratori, fornitori, consulenti, *partner* o altri soggetti terzi che operino per conto della Società e che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e al tipo di incarico da svolgere;
- attivare consulenze senza garantire congruità, adeguatezza e documentabilità dell'iniziativa;
- favorire fornitori scelti principalmente in base a criteri di amicizia, parentela o qualsiasi altra cointeressenza tale da inficiarne la validità in termini di prezzo e/o qualità ovvero che risultino strumentali alla realizzazione di una delle condotte illecite indicate nel D.lgs. n. 231/2001;

- porre in essere operazioni simulate o diffondere notizie false sulla Società e sulle sue attività;
- omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- porre in essere comportamenti che impediscano materialmente, o comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo e di revisione.

Ogni trasferimento di beni o altre utilità deve essere effettuato nel rispetto dell'operatività aziendale e in coerenza con le linee di indirizzo e le scelte strategiche definite dal CdA. In ogni caso, i soggetti aziendali (es. Amministratori, Procuratori, etc.) coinvolti (in qualità di alienante o acquirente) nel trasferimento di valori, largamente intesi, sono tenuti a verificare:

- l'identità della parte contraente nonché l'assenza di rapporti di parentela e affinità tra le parti;
- l'eventuale irrisorietà del prezzo pattuito, rispetto al valore effettivo;
- il mancato pagamento del prezzo concordato e la conseguente indisponibilità/mancata amministrazione dei valori;
- la sussistenza del patto di riscatto tra le clausole contrattuali.

La Direzione Amministrazione, Finanza e Controllo verifica, al momento della ricezione del relativo contratto, l'eventuale sussistenza di una delle condizioni di cui sopra, segnalando tempestivamente all'OdV, la tipologia di rapporto in essere nonché la condizione riscontrata nel rapporto contrattuale.

Chiunque venga a conoscenza di tali ipotesi è tenuto a segnalarle direttamente all'Organismo di Vigilanza.

Sono altresì vietate condotte volte a esercitare pressioni nei confronti delle Funzioni coinvolte nelle attività oggetto del protocollo (anche basate sul grado o sulla funzione ricoperta all'interno dell'Azienda) al fine di eludere le presenti disposizioni. È fatto obbligo di segnalare all'Organismo di Vigilanza, anche senza riferimenti a nominativi, l'eventuale esistenza di tali condotte o l'instaurarsi di prassi di questo genere.

La Società condanna tramite l'applicazione del Sistema Disciplinare i comportamenti difformi ai princìpi sopra menzionati, nonché ai presidi di controllo di seguito riportati.

7. PRESIDI DI CONTROLLO

Le modalità operative che il Personale della Società è tenuto a osservare per i processi sensibili nell'ambito delle attività di Gestione delle operazioni e degli adempimenti fiscali ai fini della prevenzione dei reati di cui al D.lgs. 231/2001 sono di seguito descritte. La Società condanna tramite l'applicazione del Sistema Sanzionatorio i comportamenti difformi alle seguenti disposizioni.

7.1 SELEZIONE DEL CONTRAENTE

La selezione dei fornitori deve avvenire secondo il principio generale di buona fede e con la diligenza ordinaria nella gestione delle attività, nel rispetto dei princìpi espressi dal Codice Etico e in applicazione della Procedura Aziendale 2.3, del Protocollo Corporate "Gestione degli

approvvigionamenti" e delle altre procedure operative, che vengono qui integralmente richiamate per quanto di competenza.
Al fine di rendere più affidabile la veridicità del corrispettivo pattuito, che rappresenta la base di calcolo dell'imposta, il processo di ricerca, selezione e qualifica dei fornitori, dovrà seguire la procedura aziendale attuale dall'azienda che si fonda su criteri oggettivi di selezione, che ne garantiscono la trasparenza.
Il rispetto dei requisiti richiesti ai fornitori è garantito tramite adeguate procedure di monitoraggio che tengono conto anche dei profili di rischio delle diverse categorie di fornitori.

Le eventuali attività sospette sono segnalate all'Organismo di Vigilanza.

7.2 STIPULA E VERIFICA DEI CONTRATTI/FORNITURA

Nella fase di conclusione del contratto, sono anticipatamente definite le modalità ed i parametri per la determinazione del prezzo, valutando altresì la congruità dello stesso rispetto ai riferimenti di mercato.
Al fine di contrastare l'instaurazione di rapporti negoziali fittizi con soggetti che non svolgono in realtà alcuna prestazione ovvero una prestazione o un servizio difforme da quello pattuito all'interno del contratto, dovrà essere debitamente archiviata e conservata la documentazione allegata al contratto (approvazione del contratto da parte dei diversi livelli autorizzativi, ordine di acquisto, documentazione di supporto, ordinativi, DDT, evidenze di comunicazioni).

Al ricevimento dei beni o alla fine dell'esecuzione degli interventi richiesti, il Soggetto richiedente la fornitura, controlla la conformità qualitativa e quantitativa del materiale consegnato con il documento di trasporto e con quanto indicato nell'Ordine di acquisto; verificata la conformità, i documenti relativi devono essere trasmessi immediatamente all'Ufficio Acquisti, quale conferma.

Solo in caso di avvenuta conferma, accertata l'effettiva erogazione delle prestazioni e/o fornitura dei servizi e l'equivalenza tra quanto indicato nei documenti contabili e quanto effettivamente nella disponibilità della società, la Direzione Amministrazione, Finanza e Controllo potrà procedere al pagamento.
Le eventuali attività sospette sono segnalate all'Organismo di Vigilanza.

7.2.1 RITENUTE E COMPENSAZIONI IN APPALTI E SUBAPPALTI

Nella concreta possibilità di monitorare ogni operazione commerciale relativa ad affidamenti in appalto, subappalto e/o a qualsiasi forma di rapporto negoziale comunque denominata, è fatto obbligo a tutti i destinatari del Modello di rispettare ogni procedura aziendale idonea ad impedire che la Società prosegua operazioni commerciali con aziende di cui non abbia:

- accertato l'effettiva esistenza (visura camerale, banche dati, sito internet);
- accertato la qualifica dei rappresentanti (titolari, legali rappresentanti, soci);
- accertato i requisiti oggettivi e soggettivi delle aziende in subappalto e/o ATI;
- approfondito eventuali ed importanti scostamenti dai prezzi standard di mercato.

7.2.2. GESTIONE DEL CICLO DI FATTURAZIONE ATTIVA E PASSIVA

Per quanto attiene al ciclo di fatturazione passiva, tutti i pagamenti vengono effettuati previa verifica dell'avvenuta autorizzazione da parte dei singoli soggetti titolari del potere di disporre spese. La Direzione amministrazione e finanza assicura che i pagamenti vengano disposti esclusivamente laddove il processo decisionale che porta alla richiesta di pagamento sia stato correttamente seguito da parte delle singole funzioni che richiedono di procedere. Laddove riscontri eventuali criticità o difformità rispetto alla procedura, ne dà comunicazione al soggetto responsabile affinché fornisca spiegazioni e ne informa gli organi di controllo, nonché l'odv nel caso in cui la difformità o l'anomalia venga successivamente sanata, procede al pagamento, archiviando copia della corrispondenza intercorsa.

Per quanto concerne il ciclo di fatturazione attiva, le "Istruzioni Operative Ufficio Contratti" hanno individuato una struttura dedicata alla gestione del contratto e del ciclo attivo di fatturazione dei servizi a canone o a consuntivo, inserito all'interno dell'Ufficio Fatturazione. La procedura individua due macro processi legati alla registrazione dei contratti ricevuti e alla fatturazione delle prestazioni ivi contenute.

Con particolare attenzione alla fatturazione passiva, occorrerà verificare la coerenza del trattamento IVA sulla base delle informazioni riportate su ordini/contratti di acquisto, documenti logistici e la fattura emessa dal fornitore. La procedura indica un'apposita sezione alle modalità di registrazione dei documenti contabili in particolare sull'utilizzo di apposite causali per identificare i vari trattamenti IVA con il duplice obiettivo di determinare correttamente l'IVA periodica (a debito o credito) ed ottenere una classificazione delle operazioni conforme, o comunque riconciliabile) a quella prevista nella dichiarazione annuale, evitando operazioni manuali di riclassificazione. Le fattispecie IVA registrate sono monitorate e controllate periodicamente.

7.3 SISTEMA E INFRASTRUTTURE IT

Il sistema informatico coinvolto nella prevenzione del rischio fiscale, consente un monitoraggio e un'informativa costante in merito alle scadenze, con meccanismi di *alert* e verifica di effettuazione degli adempimenti. L'affidabilità e la sicurezza del sistema informatico è garantito dalle seguenti procedure:

- **Procedure di protezione del sistema informatico**

  La procedura è diretta a prevenire qualsiasi manipolazione non autorizzata e garantire un sufficiente livello di protezione dei dati. La procedura comprende le modalità di controllo degli accessi ai sistemi informatici, di protezione da intrusioni non autorizzate (firewall e protezioni antivirus) nonché le modalità di archiviazione dei documenti per assicurare la conservazione in sicurezza, integrità, autenticità dei dati e tracciabilità delle registrazioni, soprattutto quelle con valore legale e per cui l'archiviazione informatica sostituisce quella cartacea.

- **Procedura di controllo dei supporti informatici (dati principali o master file)**

  Regolamenta le misure per fronteggiare i seguenti rischi:

a) registrazione errata e/o incompleta delle transazioni nel sistema contabile;
b) uso di dati permanenti errati o non aggiornati.

- **Procedure funzionamento applicativi e data base**

Si tratta di istruzioni operative contenute nelle procedure utenti dei singoli applicativi software (contabilità generale, fatturazione, contabilità di magazzino) oltre che la gestione dei data base, delle interfacce e più in generale del data quality.

- **Infrastruttura IT**

Questa procedura disciplina la separazione delle funzioni tra sviluppo, prova e funzionamento, separazione delle funzioni tra gli utenti (requisito della *Segregation of Duties*), controlli degli accessi e tracciabilità delle attività nei vari applicativi aziendali. Tali requisiti assicurati da più procedure che disciplinano le fasi di sviluppo e test del software, le misure per la sicurezza degli accessi ai sistemi, le politiche sui profili utenti etc.

Le eventuali attività sospette sono segnalate all'Organismo di Vigilanza e al Consiglio di Amministrazione.

8. CONSERVAZIONE DELLA DOCUMENTAZIONE

I Responsabili delle Funzioni/Uffici coinvolti nei processi sensibili individuati nel presente protocollo operativo sono responsabili, ciascuno per la parte di propria competenza, della conservazione della documentazione, nel rispetto dei termini di legge, al fine di garantire la tracciabilità delle operazioni aziendali.
Tutti i documenti contabili dovranno essere conservati in formato "pdf" non modificabile al fine di garantirne l'integrità e l'inviolabilità; gli *out flow* economici dovranno essere eseguiti attraverso modalità che ne consentano la tracciabilità, con la conseguenza che ogni movimentazione dovrà essere corredata da un apparato documentale che consentirà una ricostruzione *ex post* dei flussi.
La documentazione è, inoltre, messa a disposizione, su richiesta, del Presidente del CdA, del Consiglio di Amministrazione, dei Revisori dei conti, del Sindaco Unico e dell'Organismo di Vigilanza.
I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per 10 anni, salvo diverse previsioni legislative.

9. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Al fine di verificare il rispetto delle procedure relative al processo in oggetto, i Responsabili delle Funzioni interessate inviano all'Organismo di Vigilanza, con periodicità definita dallo stesso, apposite relazioni, segnalando eventuali ipotesi di anomalie verificatesi ma non oggetto di immediata segnalazione.

I Revisori dei Conti nonché il Sindaco Unico, nello svolgimento della loro attività di controllo, qualora verifichino anomalie o criticità nello svolgimento della seguente procedura, dovranno darne tempestiva comunicazione all'ODV.

Inoltre, chiunque rilevi anomalie nello svolgimento delle attività oggetto del presente Protocollo è tenuto a informare tempestivamente l'Organismo di Vigilanza sulle criticità riscontrate.

Conformemente a quanto stabilito nella Parte Generale del Modello 231, fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli di propria iniziativa o a seguito delle segnalazioni ricevute, esso effettua periodicamente controlli a campione sulle attività di "Gestione delle operazioni e degli adempimenti fiscali", diretti a verificare il rispetto delle procedure indicate.