Modello di organizzazione e gestione ex D.Lgs. 8 giugno 2001, n. 231

Engineering D.HUB S.p.A.

Versione approvata dal Consiglio di Amministrazione il 13/03/2019

N.ro versione: 4.0

N.ro pagine: 91

Nome file: DHB_Modello_di_Organizzazione_e_Gestione_231 4.0

AGGIORNAMENTI DELLA VERSIONE

Versione	Data	Motivo	Modifiche
1.0	04/08/2014	Nuova emissione	Nuova emissione
2.0	08/03/2016	Revisione complessiva	▪ Aggiornamento complessivo dovuto all'inserimento, da parte del Legislatore, di nuovi reati nell'area di applicazione del D.Lgs. 231/01 ▪ Razionalizzazione della struttura del Modello, con inserimento di Principi di comportamento di valenza generale e di valenza specifica, per tipologia di reato ▪ Incrementata la frequenza dei flussi informativi periodici verso l'Organismo di Vigilanza
3.0	21/09/2017	▪ Revisione per adeguamento alle evoluzioni legislative	▪ Introduzione dell'art. 603-*bis* c.p., come modificato dalla Legge n. 199/2016 e ricompreso nell'art. 25-*quinquies* del D.Lgs. 231/01 ▪ Inserimento nella Parte Speciale del Modello dedicata ai reati presupposto della responsabilità dell'ente, della previsione contenuta nell'art. 23 del D.Lgs. 231/01 ▪ Modifiche del reato di Corruzione tra privati ▪ Introduzione del reato di istigazione alla corruzione tra privati
		▪ Revisione per intervenuta revoca dalla quotazione delle azioni di Engineering Ingegneria Informatica S.p.A.	▪ Eliminazione delle Parti Speciali del Modello che non risultano più aderenti alla realtà della Società a seguito della revoca dalla quotazione delle azioni della Engineering Ingegneria Informatica S.p.A. intervenuta in data 8 luglio 2016
		▪ Nuovo organigramma del 16/06/2017	▪ Aggiornato §1.2.2

4.0	13/03/2019	▪ Aggiornamento del "Manuale dell'Organizzazione del Gruppo Engineering Italia" ▪ Introduzione della L. 179 del 30 novembre 2017 sul Whistleblowing ▪ Modifica dell'art. 25-duodecies del D. Lgs. 231/01 ▪ Nuovo organigramma del 21/12/2018 (Prot. 03/2018 D-HUB/AD-FB/VA/lr)	▪ Aggiornamento del paragrafo dedicato alla descrizione della struttura organizzativa della Società ▪ Introduzione del paragrafo dedicato al Whistleblowing ▪ Revisione del paragrafo dedicato al sistema disciplinare, al fine di adeguarlo alle novità legislative in materia di Whistleblowing ▪ Aggiornato §1.2.2

Sommario

1 SEZIONE GENERALE

1.1 Il Decreto Legislativo n. 231/2001

Il Decreto Legislativo 231/01 ("*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica …*", dell'8 giugno 2001) sancisce il principio per cui alcuni enti collettivi (di seguito anche "*Enti*") rispondono, nelle modalità e nei termini indicati, dei reati commessi da Personale interno alla struttura aziendale, reati specificatamente indicati dal Decreto stesso.

In un'assoluta ottica di responsabilizzazione dell'Ente per una corretta organizzazione gestionale, un valido fattore di difesa che il soggetto giuridico può spendere in caso di commissione di un reato che vede la struttura perseguire un illecito interesse o beneficiare di un indebito vantaggio, è dato dalla possibilità di dimostrare la sua assoluta estraneità istituzionale ai fatti criminosi, con conseguente emersione di responsabilità e/o interesse esclusivamente in capo al soggetto agente che ha commesso l'illecito.

La suddetta estraneità va comprovata attraverso la funzionalità di un'organizzazione interna attenta, in chiave di prevenzione, sia alla formazione della corretta volontà decisionale della struttura sia alla vigilanza circa il corretto utilizzo delle risorse finanziarie aziendali.

Con il D.Lgs. 231/2001 è stato quindi recepito nel nostro ordinamento il principio per cui anche le persone giuridiche rispondono in modo diretto dei reati commessi, nel loro interesse o a loro vantaggio, da chi opera professionalmente al loro interno.

La sanzionabilità dell'Ente e la correlata funzionalità complessiva del sistema preventivo, atto a scongiurare l'addebito di responsabilità, sono concetti legati alla capacità di lettura dell'organizzazione interna della persona giuridica e della conseguente corretta costituzione sia di norme etiche preventive che delle regole di sorveglianza "difensiva" sui fatti (quali per l'appunto, quelle contenute nei "*Modelli di organizzazione e di gestione*"), che gli amministratori hanno l'obbligo civilistico di precostituire anche nell'interesse del patrimonio sociale.

La suddetta verifica passa anche attraverso:

- le misure di vigilanza interna sui "modelli di organizzazione e gestione" istituiti;
- la costituzione di appositi organi dotati di adeguati poteri;
- il riscontro della sussistenza o meno di caratteri elusivi specifici verso le suddette misure, nei fatti occorsi, da parte di coloro che, nonostante le misure preventive, hanno commesso i reati.

L'essenza della normativa in oggetto comporta che se il reato è commesso da persone "*appartenenti*", nei termini appositamente stabiliti dal Decreto, alla persona giuridica, la commissione di quel reato comporta anche direttamente, in aggiunta alle conseguenze "tipiche" che procurerà a carico del reo, l'applicabilità consequenziale di diverse e gravi sanzioni direttamente a carico della Società.

L'effetto pratico primario del Decreto è, quindi, l'ampliamento dello spettro di responsabilità per il compimento di certi reati.

L'aver beneficiato, anche economicamente, di un illecito è presupposto valido per scontare le responsabilità consequenziali previste dalla legge, che affiancano e non sostituiscono le eventuali conseguenze di tipo civilistico, ovvero quelle basate su impatti di danno verso terzi.

Tale riverbero di responsabilità sorge allorché certe persone appartenenti professionalmente all'Ente si rendono autrici di certi specifici reati, in seguito detti anche "*reati-presupposto*".

Dunque la tematica implica a monte un'analisi selettiva sia sui Soggetti che determinano la responsabilità sia sugli illeciti che comportano l'insorgenza della stessa.

Quanto ai predetti Soggetti "interni", la legge dispone che si tratta dei seguenti:

1. persone che rivestono funzioni di rappresentanza;
2. persone che rivestono funzioni di amministrazione;

3. persone che rivestono funzioni di direzione dell'Ente o di una sua unità organizzativa autonoma (una sede secondaria, ad esempio, ma anche uno stabilimento o una rappresentanza);
4. persone che esercitano anche di fatto la gestione o il controllo dell'Ente stesso;
5. persone sottoposte alla direzione o alla vigilanza di qualunque Soggetto menzionato nei punti precedenti (il che corrisponde ad un'estensione cospicua dell'ambito soggettivo in parola).

Il Decreto dispone che la responsabilità dell'Ente non scatta se risulta dimostrato processualmente che le persone fisiche sopra elencate hanno commesso il reato che ha determinato l'implicazione derivata della persona giuridica operando esclusivamente nell'interesse proprio o di terzi estranei.

Due le tipologie soggettive dei Soggetti interni rilevanti: apicali e sottoposti.

La posizione apicale è in sostanza quella che dà luogo alle ipotesi che più sopra abbiamo incluso nei punti da 1 a 4. È infatti a quei Soggetti che, nell'ambito del decreto, è destinata con priorità la disciplina della capacità esimente di quello che chiamiamo, più avanti, con termine già in voga nella prassi, lo "scudo protettivo" (cioè il compendio di misure volte a prevenire la "trasmissione" di responsabilità che è il punto nodale del Decreto). Per ciò che attiene al rapporto tra Soggetti "apicali" e "scudo", è importante sottolineare come, perché lo "scudo" risulti efficace, in caso di reati commessi da questi Soggetti, è necessario dimostrare in giudizio che nel commettere il reato costoro hanno agito con dolo anche verso lo *scudo*, cioè si sono volontariamente e fraudolentemente sottratti alle prescrizioni e ai contenuti del "*Modello di organizzazione e gestione*".

Va altresì dimostrato, oltre a ciò che attiene all'azione dei "trasgressori", che non vi è stata omessa o insufficiente sorveglianza da parte dell'apposito "Organismo di Vigilanza" in ordine al funzionamento, all'osservanza ed all'aggiornamento del Modello.

Per i Soggetti sottoposti alla direzione di altri (i Dipendenti o i Collaboratori non apicali), fermo che anche essi non trasmettono all'Ente responsabilità se agiscono, col reato, nell'interesse esclusivo proprio o di terzi, la responsabilità è ascrivibile all'Ente solo se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza, cosa che è esclusa presuntivamente, dall'adozione ed efficace attuazione, prima della commissione del reato, di un modello *idoneo a prevenire reati della stessa specie di quello verificatosi*.

Per quanto riguarda i reati da cui discende la responsabilità degli Enti (di seguito, spesso, anche "*reati-presupposto*"), il decreto legislativo 231/2001 individua le seguenti tipologie omogenee:

a) indebita percezione di erogazioni, truffa in danno dello Stato o di un Ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un Ente pubblico
b) reati informatici e trattamento illecito di dati
c) delitti di criminalità organizzata
d) concussione, induzione indebita a dare o promettere utilità e corruzione
e) falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento
f) delitti contro l'industria e il commercio
g) reati societari
h) delitti con finalità di terrorismo o di eversione dell'ordine democratico
i) pratiche di mutilazione degli organi genitali femminili
j) delitti contro la personalità individuale
k) abusi di mercato
l) omicidio colposo o lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
m) ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
n) delitti in materia di violazione del diritto d'autore
o) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
p) reati ambientali
q) impiego di cittadini di paesi terzi il cui soggiorno è irregolare
r) razzismo e xenofobia

s) ***reati transnazionali*** (favoreggiamento personale, contrabbando di tabacchi lavorati esteri, immigrazioni clandestine.)

Si segnala, inoltre, che, nella generalità dei casi e ad eventuale integrazione di sanzioni di altro tipo, l'Ente ritenuto responsabile per il compimento di un determinato reato può essere soggetto ad una o più delle seguenti *sanzioni interdittive*:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) divieto di pubblicizzare beni o servizi.

Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo *unico* o *prevalente* di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità è sempre disposta l'interdizione definitiva dall'esercizio dell'attività.

Si segnala, infine, che ai sensi dell'articolo 23 del D. Lgs. 231/01 "*1. Chiunque, nello svolgimento dell'attività dell'ente a cui è stata applicata una sanzione o una misura cautelare interdittiva trasgredisce agli obblighi o ai divieti inerenti a tali sanzioni o misure, è punito con la reclusione da sei mesi a tre anni. 2. Nel caso di cui al comma 1, nei confronti dell'ente nell'interesse o a vantaggio del quale il reato è stato commesso, si applica la sanzione amministrativa pecuniaria da duecento e seicento quote e la confisca del profitto, a norma dell'articolo 19. 3. Se dal reato di cui al comma 1, l'ente ha tratto un profitto rilevante, si applicano le sanzioni interdittive, anche diverse da quelle in precedenza irrogate*".

1.2 La Società Engineering. D.HUB

Engineering.MO S.p.A. nasce dall'acquisizione, da parte di Engineering, della società T-Systems Italia S.p.A., precedentemente interamente partecipata da T-Systems International GmbH.

Nel mese di settembre 2016 Engineering.MO ha acquisito il ramo di azienda di Engineering Ingegneria Informatica S.p.A. dedicato alla gestione della struttura dei Data Center, delle infrastrutture IT e delle attività operative.
Il 26 luglio 2017 l'Assemblea Straordinaria dei Soci delibera il cambiamento della denominazione sociale che diventa appunto Engineering. D.HUB S.p.A.

1.2.1 *Sistema di Governance*

Engineering. D.HUB S.p.A. (o "*la Società*" o "*l'Azienda*") ha adottato il sistema di *governance* tradizionale, che prevede i seguenti organi di amministrazione e controllo:

- *Consiglio di Amministrazione*
- Collegio Sindacale.

1.2.2 *Struttura organizzativa*

La struttura organizzativa di Engineering è articolata per aree di business secondo un modello strutturato in una Direzione Generale, all'interno del quale ogni sede operativa, fruendo di adeguati livelli di autonomia gestionale, è chiamata a presidiare uno o più segmenti di mercato.

La *Direzione Generale* è composta da più strutture tecniche subordinate (Direzioni di produzione) e affiancata da più Direzioni Generali commerciali (Direzioni Commerciali), tutte gerarchicamente subordinate all'Amministratore Delegato.

Nell'ambito della struttura tecnica, all'interno delle singole unità produttive, la responsabilità delle singole commesse è affidata ai *Capi Progetto/Service Manager*. In Engineering operano le seguenti Direzioni Generali:

- *Direzione Generale Finanza* (mercato bancario ed assicurativo)
- Direzione Generale Pubblica Amministrazione e Sanità (di seguito anche "Direzione Generale P.A. e Sanità": Amministrazioni pubbliche centrali e locali, Aziende pubbliche ed Istituzioni Comunitarie, Aziende ospedaliere e sanitarie, Policlinici universitari)
- Direzione Generale Energy & Utilities e TELCO (mercato delle utilities: elettricità, gas, igiene ambientale; fornitura di soluzioni e servizi per i principali carrier internazionali delle telecomunicazioni)
- Direzione Generale Industria e Servizi (industria metallurgica, chimica, farmaceutica, automotive, prodotti di consumo, trasporti, servizi, ecc.).

Questa premessa è stata necessaria per inquadrare la recente evoluzione organizzativa di Engineering.MO che dopo il conferimento del ramo d'azienda Managed Operation di Engineering e la nuova denominazione in Engineering D.HUB è diventata la società del Gruppo Engineering che offre servizi tecnologici e infrastrutturali a tutti i settori di mercato, con un ampio spettro di soluzioni, flessibilità nel modello operativo e una competenza su scenari e processi dei singoli clienti maturata in oltre 20 anni di esperienza nel campo delle Managed Operations.

L'offerta di E.D.HUB è focalizzata nell'ambito della gestione di infrastrutture tecnologiche, e transita da una rete integrata di Data Center dislocati sul territorio nazionale ad Aosta (Pont-Saint-Martin), Milano, Torino e Vicenza e per risponde ai più elevati standard di sicurezza.

L'Organizzazione è orientata alla costante evoluzione delle soluzioni tecnologiche proposte al parco Clienti Engineering.

L'organigramma di Engineering D.HUB si articola sotto la guida di una Amministratore Delegato nelle seguenti direzioni:

- *Business Operations: Struttura finalizzata* al supporto della governance economica dell'organizzazione ed alla definizione e all'implementazione dei processi trasversali all'organizzazione in armonia con quanto definito dal gruppo Engineering
- *Transformation*
- *Information Lead*
- *Technology Office*

E una struttura di Delivery che si articola in 6 Direzioni:

- *Solutions, Portfolio & Business Development:* Struttura responsabile del disegno e dello sviluppo del portafoglio di offerta dell'azienda. Sotto la sua responsabilità ricade il solutioning delle nuove opportunità e dei principali rinnovi contrattuali.
- *Sales Specialists:* Struttura preposta alla gestione commerciale del portafoglio di offerte DHUB. Opera sia in autonomia sia in cooperazione con le funzioni commerciali di Mercato al fine di estendere il Business.
- *Clients & Project Management:* Organizzazione finalizzata alla gestione dei contratti in essere. Responsabile del P&L del portafoglio Clienti assegnato nonché dello sviluppo di nuove opportunità.
- *Cloud & Technology Services:* Struttura di delivery responsabile dell'erogazione di servizi Data Center Tradizionali, servizi sistemistici e di gestione on-site e on-center e di servizi innovativi principalmente, ma non solo, basati sul Cloud.
- *Business & User Services*: Struttura di Delivery responsabile dell'erogazione di servizi legati all'utenza finale, come Service Desk, Fleet Management e Digital workplace.

- *Cyber Security Services:* Struttura di delivery finalizzata all'erogazione dei servizi legati agli aspetti di sicurezza interna e verso i clienti finali sia in tandem con le strutture di delivery sopra indicate sia attraverso specifici progetti dell'ambito della Cyber Security

Ad integrazione della struttura organizzativa appena descritta, operano le seguenti Direzioni centralizzate a livello di Gruppo:

- *Direzione Generale Amministrazione Finanza e Controllo*
- *Direzione Generale Human Resource & Organization*
- *Direzione Generale Tecnica, Innovazione e Ricerca*
- *Direzione Formazione*
- *Coordinamento Privacy*
- *Direzione Processi e Audit Interni.*

Di seguito vengono fornite ulteriori sintetiche informazioni inerenti alcune delle citate Direzioni.

La Direzione Generale Amministrazione Finanza e Controllo è strutturata nelle seguenti Unità Organizzative (in seguito anche "*UU.OO.*"):

- Direzione Amministrativa
- Centro Servizi Amministrativi
- Direzione Bilancio Capogruppo
- Servizi Bilancio D.Hub e altre Partecipate Italiane
- Direzione Bilanci Partecipate Estere
- Direzione Bilanci Partecipate Italiane
- Direzione Controllo di Gestione di Gruppo
- Direzione Affari Legali e Societari
- Direzione Acquisti e Affari Generali
- Direzione Ufficio Gare
- Gestione dei Contratti
- Direzione Acquisti Consulenze Informatiche
- Dir. Amministrazione del Personale
- Controller di Area
- Direzione Servizi Finanziari
- Progetto Crediti
- Servizi Fiscali
- M&A.

- La Direzione Generale *Human Resource & Organization* è strutturata nelle seguenti UU.OO.:

- Direzione Relazioni Industriali
- Direzione Risorse umane Area Nord
- Direzione Risorse umane Area Centro Sud

- Direzione Compensation & Benefits, International Mobility
- Coordinamento Privacy
- Servizio Piani Provvigionali
- Direzione Sistema Informativo Interno
- Servizio Salute & Sicurezza e Ambiente..

- La *Direzione Generale Human Resource & Organization* è inoltre responsabile della gestione e del mantenimento della certificazione ISO 14001 del Sistema per la Gestione Ambientale.

La Direzione Generale Tecnica Innovazione e Ricerca, oltre ad attività di progettazione di alto profilo innovativo, gestisce i progetti di ricerca finanziati, totalmente o parzialmente, dall'Unione Europea o da altri Enti Pubblici.

La Direzione Generale è strutturata nelle seguenti Direzioni:

- Direzione Ricerca e Sviluppo
- Direzione ERP/Business Development
- Direzione ESL Excellence Centre
- Direzione *Engineering Software Laboratories*
- Direzione Sviluppo Offerta.

- alla Direzione Engineering Software Laboraties riportano le seguenti Direzioni;

- Dir. Metodologie, Processi e Servizi ESL
- Dir. ESL AM, Progetti Internazionali e CC HOST
- Dir. ESL Progetti & Consulenza;

- alla Direzione ESL Excellence Centre riportano le seguenti Direzioni:

- Direzione Data&Analytics exc
- Direzione PM/PMO/exc
- Direzione Fonderie Multimediali
- Direzione Architet. e Sistemi Intelligenti
- Direzione CC ECM;

- alla Direzione ERP/Business Development riporta la:

- Direzione Tecnica ERP.

Nell'ambito della Direzione Processi e Audit Interno opera il *Servizio di Internal Auditing*. Il suo principale compito è quello di attuare un controllo sul rispetto dei protocolli previsti dal presente *Modello* da parte delle varie UU.OO. della Capogruppo e delle varie Società controllate, al fine di garantire:

- l'affidabilità e l'integrità delle informazioni contabili, finanziarie ed operative
- l'efficacia e l'efficienza delle operazioni

- la salvaguardia del patrimonio
- la conformità a leggi, regolamenti e contratti.

L'*Internal Auditing* è anche tenuto a riportare le principali evidenze e criticità emerse sia all'attenzione del Top Management della Società e su richiesta agli organi di controllo e vigilanza: *Collegio Sindacale* e *Organismo di Vigilanza* (ex D.Lgs. 231/01; vedasi successivamente "*L'Organismo di Vigilanza*").

La *Direzione* Processi e Audit Interno è, inoltre, responsabile:

- della gestione e del mantenimento delle certificazioni acquisite dalla Società:
  - ✓ UNI EN ISO 9001:2015 – Sistema Qualità
  - ✓ ISO-IEC 20000–1:2011 – Gestione dei Servizi ICT
  - ✓ ISO-IEC 27001:2013 – Gestione Sicurezza delle Informazioni

  compreso quindi lo svolgimento di periodiche visite ispettive interne alle varie UU.OO. della Società;
- della manutenzione delle procedure e dei documenti aziendali di riferimento nell'ambito dei sistemi certificati.

Come sopra anticipato, la gestione e il mantenimento della certificazione ISO 14001 del Sistema per la Gestione Ambientale sono, invece, di competenza della *Direzione Generale Human Resource & Organization*

1.2.3 ***Company Profile***

Engineering (che comprende Engineering D.HUB) è il maggiore gruppo italiano di Information Technology, con un'offerta completa e integrata di *system integration & consulting, managed operations*, consulenza e soluzioni verticali.

La Capogruppo *Engineering - Ingegneria Informatica S.p.A.*, costituita nel 1980, è stata quotata al TechSTAR, il segmento di Borsa dedicato ai titoli con alti requisiti patrimoniali e finanziari, fino al luglio 2016, quando è stata completata la procedura di OPA con la conseguente revoca dalla quotazione delle azioni della Società.

Il *Gruppo Engineering* ha circa 9.000 Dipendenti dislocati in circa 50 sedi in Italia e all'estero, un portafoglio di mille Clienti ed attività IT in tutti i *verticals* di mercato: Finanza, Pubblica Amministrazione Centrale, Locale e Sanità, Industria e Servizi, Telecomunicazioni e Media, Utilities.

Per una descrizione aggiornata e più dettagliata del Gruppo Engineering si rimanda al "*Profilo di Gruppo*" reperibile al portale internet del Gruppo (**www.eng.it**), sezione: *Gruppo*.

La Società Engineering D.HUB S.p.A. non è mai stata sottoposta a procedimento ai sensi del D.Lgs. 231/01.

1.3 Il Codice Etico del Gruppo Engineering

Il *Codice Etico del Gruppo Engineering*, partendo dal patrimonio di valori condiviso da tutte le Società del Gruppo, detta le norme di comportamento che tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, instaurino a qualsiasi titolo rapporti di collaborazione od operino nell'interesse del Gruppo, devono applicare nella conduzione degli affari e nella gestione delle attività aziendali.

Il *Codice Etico del Gruppo Engineering* è da intendersi, quindi, vincolante per Amministratori, Dirigenti e Dipendenti tutti, membri degli organismi di Controllo (*Collegio Sindacale*), membri dell'Organismo di Vigilanza, Collaboratori esterni temporanei o continuativi, Partner, Fornitori e Clienti.

Il *Codice Etico del Gruppo Engineering* è parte integrante e sostanziale del presente *Modello di Organizzazione e Gestione*. Pertanto violazioni delle disposizioni in esso contenute rappresentano vere e proprie violazioni del *Modello*, con tutte le conseguenze da ciò derivanti in tema di applicabilità delle sanzioni disciplinari.

1.4 Il Modello di organizzazione e gestione ex D.Lgs 231/01 della Società

Un sistema di controlli preventivi ritenuto idoneo a garantire che i rischi di commissione dei reati previsti dal D.Lgs 231/01 siano ridotti ad un "livello *accettabile*" è quel sistema che costringe, per il suo aggiramento, ad un *comportamento fraudolento* da parte di chi compie l'atto illecito.

Il sistema suddetto si articola in specifici protocolli settoriali (*procedure*) costituiti da un insieme di controlli preventivi e successivi, parte integrante del *Modello di organizzazione e gestione* e indispensabile strumento destinato a guidare le attività dei Soggetti "sensibili".

Si ritiene che il *Modello di organizzazione e gestione* realizzato si connoti come un efficace sistema di controllo preventivo, contraddistinto dall'esistenza delle seguenti caratteristiche, che integrano fondamentali *princìpi di controllo*:

- sistema organizzativo sufficientemente formalizzato con specifico riferimento alle attribuzioni di funzioni, responsabilità e linee di dipendenza gerarchica;
- separazione, indipendenza ed integrazione fra funzioni aziendali: le varie fasi di uno stesso processo (esecuzione, controllo operativo, contabilizzazione, supervisione, autorizzazione, ecc.) non possono essere lasciate all'autonoma gestione di una singola persona;
- poteri autorizzativi e di firma formalizzati e coerenti con le funzioni e le responsabilità aziendali ricoperte dai Soggetti apicali
- punti di controllo manuali ed informatici;
- verificabilità, documentabilità e congruità di ogni processo aziendale, in particolare delle transazioni e delle operazioni più significative
- verificabilità, documentabilità delle attività di controllo: *operativo* (previsto nell'ambito del processo) o *di supervisione* (di primo e secondo livello, dove previsto)
- comunicazione continuativa all'Organismo di Vigilanza delle informazioni concernenti le operazioni a rischio e tempestiva informativa allo stesso Organismo di anomalie o violazioni del Modello organizzativo
- monitoraggio da parte dell'Organismo di Vigilanza sull'attuazione del Modello organizzativo.

1.4.1 Documenti aziendali integrati nel Modello

Vanno considerate parti integranti e sostanziali del presente *Modello di organizzazione e gestione*, anche in relazione alle conseguenze in tema di applicazione delle sanzioni disciplinari conseguenti all'eventuale violazioni delle disposizioni in essi contenute, i seguenti documenti aziendali:

- *Codice Etico del Gruppo Engineering* (già precedentemente richiamato)
- il *Manuale del Sistema di Gestione della Sicurezza dei Lavoratori*
- le Procedure, i Protocolli, i Regolamenti e le Linee Guida aziendali referenziati dai citati documenti e quelli puntualmente richiamati dal presente *Modello*

tutti reperibili nella intranet aziendale (se non di pubblico accesso al portale internet del Gruppo **www.eng.it**, alla sezione "*Investor Relations*" - "*Corporate Governance*").

1.4.2 Metodologia di definizione e revisione del Modello

Di seguito si fornisce una descrizione sintetica delle fasi operative svolte per la definizione del primo impianto del *Modello di organizzazione e gestione*, con un accenno anche alle successive fasi di revisione. In particolare ci si concentra nella descrizione dei passi seguiti per la stesura della seconda Sezione del presente *Modello*, la *Sezione speciale*, che descrive, contestualizzandolo nell'Azienda, ciascun reato-presupposto, fornendo riferimenti alle norme, ai protocolli e ai controlli posti a presidio del rischio di commissione del reato.

1.4.2.1 Analisi del reato-presupposto e individuazione della possibile modalità di commissione

Il Decreto Legislativo 231/2001 disciplina la responsabilità di un *Ente* (persone giuridiche, società e associazioni anche prive di personalità giuridica) a fronte di illeciti amministrativi dipendenti dal compimento di specifici reati. I "*reati-presupposto*" elencati dal Decreto, fin dalla sua emanazione, sono vari e sono stati successivamente integrati, a più riprese, con l'aggiunta, da parte del Legislatore, di ulteriori nuove casistiche.

Nell'approccio seguito per la definizione del *Modello di organizzazione e gestione* il primo obiettivo che ci si è posti è stato quello di identificare i rischi effettivi di commissione del reato a cui la Società era esposta.

Ciò ha richiesto innanzitutto, un'attenta analisi *tecnico-giuridica* dei reati richiamati dal Decreto. Tale processo è stato, infatti, valutato come indispensabile presupposto per la concreta identificazione dei rischi effettivamente rilevabili in Azienda, essendo questo, come sopra accennato, il nostro primo obiettivo.

Il passo successivo alla concreta identificazione del comportamento delittuoso evocato dal Decreto è stato quello di riconoscere, in qualche caso anche esercitando un certo sforzo "di immaginazione", quali potessero essere le modalità e le circostanze con le quali una o più Persone, operative nell'ambito dell'organizzazione dell'Azienda, potessero fare *proprio* il comportamento delittuoso.

All'esito dell'analisi dei rischi è stato ritenuto opportuno non inserire nel Modello le Parti Speciali relative alle ipotesi di reato presupposto che non risultano concretamente realizzabili nel contesto aziendale (come, ad esempio, la fattispecie di "pratiche di mutilazione degli organi genitali femminili" di cui all'art. 583-bis c.p. richiamato dall'art. 25-quater1 del Decreto).

1.4.2.2 Individuazione dei processi, dei Soggetti e delle UU.OO. sensibili

A partire dall'identificazione (a volte anche *astratta*) delle modalità di commissione di uno specifico reato-presupposto, esito della fase precedente, si è passati al riconoscimento, sostanzialmente concomitante:

- dei processi e dei sotto-processi aziendali in cui più facilmente può trovare modo di concretizzarsi il comportamento delittuoso;
- dei Soggetti e/o delle UU.OO. più esposte o "sensibili" al rischio di commissione del reato.

Questa fase, sostanzialmente finalizzata alla *mappatura* dei rischi, da una parte, e dei processi e delle UU.OO. sensibili, dall'altra, s'è rivelata assai efficace anche in quanto ha fornito elementi ad integrazione ed arricchimento della fase precedente. Spesso, infatti, da un'analisi più dettagliata dei processi svolti presso singole funzioni aziendali è venuta evidenziandosi una nuova modalità di possibile commissione di un reato, precedentemente non rilevata, e, a partire da questa, sono emersi nuovi processi e nuove UU.OO. *sensibili*, precedentemente sfuggiti all'analisi.

L'iterazione ciclica fra queste due prime fasi ha così consentito di raggiungere una mappatura sufficientemente accurata, risultato difficilmente raggiungibile ([1]) laddove tali fasi fossero state eseguite, in sequenza, una sola volta.

1.4.2.3 Verifica del livello di presidio dei processi a rischio

Raggiunta una visione sufficientemente completa:

- dei rischi effettivi (di commissione di un reato-presupposto) a cui l'Azienda risulta esposta,
- dei processi, dei Soggetti e delle UU.OO. *sensibili* a tali rischi

si è infine passati ad analizzare quale livello di "protezione dai rischi" venisse offerto dalle norme e dalle *procedure* aziendali esistenti. (Di seguito con il termine "*procedure*" si farà riferimento sia ai documenti che regolano specifici processi aziendali, sia, sinteticamente, all'insieme dei protocolli descritti e prescritti all'interno di tali documenti).

Va detto che data la natura dei reati richiamati dal Decreto, per molti di loro è risultato del tutto appropriato richiamare, in primo luogo, i *princìpi*, le *norme di comportamento* e i *valori* espressi nel *Codice Etico del Gruppo Engineering*, per alcuni reati-presupposto, "scudo" di per sé sufficiente a scongiurare il compimento di reati particolarmente esecrabili, connotati da un elevato disvalore sociale.

Nella generalità dei casi, eventualmente a integrazione di tale richiamo al Codice Etico, per ogni processo rivelatosi sensibile ad uno specifico rischio di reato è stata effettuata una ricognizione delle procedure aziendali esistenti, per verificare *se* ed *in quale misura* esse offrivano una sufficiente *protezione* in termini di norme e di controlli prescritti, sia *preventivi* che, eventualmente, *successivi* allo svolgimento di un determinato processo aziendale o di una sua fase.

Nei casi in cui tale protezione è risultata assente (o è stata ritenuta insufficiente), si è proceduto ad aggiornare e ad emettere nuove versioni delle procedure interessate, così da renderle idonee a proteggere rispetto al rischio specifico.

In alcuni casi, laddove, pur a fronte di una protezione insufficiente, non s'è tuttavia ritenuto opportuno provvedere, ad esempio, all'emissione di una specifica procedura, le norme e i controlli necessari a proteggere dal rischio di commissione di un determinato reato sono stati direttamente inseriti, *con pari efficacia prescrittiva*, nella *Sezione speciale* del presente *Modello di organizzazione e gestione*.

All'esito della ricognizione delle procedure aziendali e con riferimento ad uno specifico reato, è emerso che i protocolli e i controlli efficaci (anche *indirettamente*) contro il rischio di commissione del reato sono spesso molto numerosi e dettagliatamente descritti. Per migliorare la leggibilità del *Modello* s'è scelto di raggruppare protocolli e controlli, così dettagliati, in gruppi omogenei per affinità di contesto e di finalità, sintetizzandoli, ciascun gruppo, in una *descrizione sintetica* di norme, protocolli e controlli (vedi seguito), descrizione identificata nel *Modello* dal codice "*Id. Protoc.*".

Il contenuto dettagliato di un determinato protocollo (riportato nel *Modello*) - e dei relativi controlli - è sempre disponibile:

- accedendo ai documenti aziendali di riferimento, puntualmente indicati;
- consultando un voluminoso documento (ad uso interno) che espone, per ciascun "*Id. Protoc.*" citato nel *Modello*, i protocolli ed i controlli di dettaglio prescritti in Azienda.

Con riferimento a questo secondo punto, va sottolineato che il citato documento, ad uso interno:

- viene mantenuto costantemente aggiornato;
- contiene controlli di dettaglio che sono presi in esame dall'Internal Auditing nello svolgimento delle sue attività istituzionali, verificandone l'effettiva attuazione, anche a beneficio dell'Organismo di Vigilanza.

([1]) … anche facendo leva, così com'è avvenuto, sul possesso di una profonda conoscenza dell'organizzazione aziendale da parte delle persone che hanno svolto tale analisi. Ciò a causa della molteplicità di funzioni e di processi riscontrabili in un'Azienda di grandi dimensioni come è Engineering. D.HUB.

In conclusione, nella *Sezione speciale* del *Modello*, sono stati quindi riportati, per ciascun reato-presupposto:

- la *descrizione sintetica del reato* e, laddove necessario, alcune esemplificazioni dello stesso
- la *contestualizzazione aziendale*: processi/UU.OO. sensibili e possibili modalità di commissione
- la *descrizione del comportamento aziendale prescritto,* delle norme e dei protocolli
- la *descrizione sintetica dei controlli applicati*
- *i riferimenti ai documenti aziendali* contenenti le norme ed i protocolli.

1.4.2.4 Revisione del Modello

Il presente *Modello di organizzazione e gestione* è soggetto a periodiche verifiche, soprattutto in ottica di efficacia rispetto agli obiettivi per i quali è stato predisposto e di garanzia di effettiva attuazione di quanto previsto dal *Modello* stesso. In questa attività di verifica il ruolo principale è svolto dall'*Organismo di Vigilanza* (istituto di seguito dettagliatamente descritto), che potrà avvalersi, in proposito, dell'apporto informativo a lui fornito dalla *Direzione* Processi e Audit Interno.

Eventi che possono determinare la revisione del *Modello* sono i seguenti:

- il manifestarsi di significative violazioni delle prescrizioni contenute nel *Modello* (o nelle procedure da esso richiamate), tali da evidenziare, anche indirettamente, una vulnerabilità rispetto al rischio di commissione di un determinato reato;
- variazioni intervenute nell'organizzazione dell'Azienda o nei processi aziendali, laddove le une e/o le altre richiedano un aggiornamento della "mappatura" delle tre entità: rischio da reato – Soggetti o UU.OO. sensibili – processi/sottoprocessi sensibili e, conseguentemente, una verifica delle norme, dei protocolli e dei controlli da prevedere a protezione del rischio;
- modifiche o integrazioni al D.Lgs. 231/01 attuate dal Legislatore, con introduzione di nuovi reati-presupposto (precedentemente non compresi nell'ambito) o con interventi di modifica rispetto a reati già previsti dal Decreto.

In tutti i casi, a prescindere dalla motivazione che ha innescato il processo di revisione del Modello, vengono replicate le tre fasi operative che hanno portato alla prima stesura del Modello, già precedentemente descritte.

Ogni intervento di revisione del *Modello* sarà ovviamente seguito dalle fasi di approvazione e pubblicazione di seguito trattate.

Si precisa che *non* costituisce "*revisione del Modello*" la semplice modifica di uno o più dei documenti da esso richiamati (referenziati nella *Sezione speciale* del presente documento). Coloro che, nell'applicazione di quanto previsto dal presente Modello, si trovano a dover far riferimento ai documenti da esso richiamati, sono tenuti ad accedere all'ultima versione degli stessi disponibile all'interno della intranet aziendale.

1.4.3 Approvazione del Modello e sua pubblicazione

Ai fini della sua promulgazione, il presente *Modello di organizzazione e gestione* è soggetto all'approvazione del Consiglio di Amministrazione della Società ("*CdA*").

In occasione di una revisione del *Modello*, laddove le modifiche apportate non rivestano caratteristiche di particolare urgenza, tale approvazione interverrà in occasione del primo *CdA* utile. Diversamente l'Amministratore Delegato, eventualmente su sollecitazione dell'*Organismo di Vigilanza* o del Responsabile della *Direzione* Processi e Audit Interno, convocherà anticipatamente un apposito *CdA* per l'approvazione della nuova versione del Modello.

Una volta approvato, il *Modello di organizzazione e gestione* viene pubblicato all'interno della rete intranet aziendale.

La promulgazione di una nuova versione del *Modello* viene sempre accompagnata da una contestuale comunicazione interna, via e-mail, destinata a tutti i Dipendenti, con la quale si segnala la disponibilità della nuova versione nella intranet aziendale e si precisano, sinteticamente, le ragioni che hanno motivato l'aggiornamento.

1.4.4 Destinatari e ambito d'applicazione del Modello

Il Decreto sancisce che l'Ente è ritenuto responsabile nel caso di reati commessi nel suo interesse o a suo vantaggio dai seguenti Soggetti:

- Persone che rivestono funzioni di rappresentanza o di amministrazione;
- Persone che rivestono funzioni di direzione dell'Ente o di una sua Unità Organizzativa autonoma (ad esempio, di una sede secondaria);
- Persone che esercitano, anche di fatto, la gestione o il controllo dell'Azienda;
- Persone sottoposte alla direzione o alla vigilanza di qualunque Soggetto menzionato nei punti precedenti.

Oltre a tali Destinatari, prevalentemente, ma non *necessariamente* Dipendenti dell'Azienda, tutti comunque operanti nell'ambito delle attività svolte dall'organizzazione aziendale, sono tenuti a conformarsi alle norme e ai princìpi richiamati dal presente *Modello* tutti coloro che instaurano relazioni con Engineering D.HUB (regolate o meno da un rapporto contrattuale): Clienti, Partner e Fornitori.

In particolare si sottolinea che i princìpi, le norme ed i protocolli richiamati dal presente *Modello* devono essere osservati anche nell'ambito di attività svolte all'estero, in nome o per conto di *Engineering D.HUB S.p.A*.

1.5 L'Organismo di Vigilanza

1.5.1 Presupposti alla sua istituzione

Il D.Lgs. 231/2001 prevede che l'adozione di un modello di organizzazione e gestione sia accompagnata dalla individuazione ed istituzione di un apposito *Organismo di Vigilanza* (di seguito anche "*OdV*").

Più precisamente, tale organismo è disciplinato dall'articolo 6 del decreto in questione, ai sensi del quale l'Ente non risponde dei reati eventualmente compiuti anche o solo nell'interesse o a vantaggio dell'Ente stesso, qualora quest'ultimo dia prova, tra l'altro, (a) che è stato preventivamente adottato un valido modello di organizzazione; (b) che "*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*".

In sostanza, in base al citato articolo 6, il c.d. "*scudo protettivo*" che dovrebbe mettere l'Ente al riparo dalle conseguenze derivanti dal compimento di un reato da parte di un Soggetto che riveste al suo interno una posizione *apicale* (così come definita dal Decreto), risulta realizzato, oltre che da un valido modello di organizzazione e gestione, anche dalla istituzione di un idoneo *Organismo di Vigilanza*.

Per quanto, invece, riguarda i reati compiuti dai c.d. Soggetti *non apicali* (così come definiti dall'articolo 5, comma 1, lett. b, del D.Lgs 231/01), si deve segnalare che non è richiesta con altrettanta chiarezza l'individuazione o l'istituzione di tale organismo di controllo. In realtà, però, si deve rilevare che l'articolo 7 del medesimo decreto, che appunto disciplina i reati compiuti dai Soggetti non apicali, prevede che il modello, per poter validamente proteggere l'Ente, debba essere efficacemente attuato, precisando poi che l'efficace attuazione del modello richiede, tra l'altro, "*una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività*". È chiaro, quindi, che tale periodica verifica non potrà che essere svolta da un idoneo Organismo di Vigilanza.

1.5.2 Requisiti dell'OdV e dei singoli membri, cause d'ineleggibilità e di decadenza

Di seguito si descrivono i requisiti che, sulla base dell'interpretazione del art. 6 del D.Lgs. 231/01, devono caratterizzare un Organismo di Vigilanza:

a) **Autonomia e indipendenza**: l'Organismo deve essere dotato di autonomia ed indipendenza rispetto agli organi direttivi dell'Ente, in modo da poter svolgere al meglio il suo ruolo. Tale autonomia e indipendenza non richiedono soltanto l'assenza di ogni forma di subordinazione gerarchica, ma anche il mancato conferimento di poteri operativi e decisionali. Infatti, la presenza di tali poteri in capo all'organismo potrebbe, in alcuni casi, pregiudicare e compromettere i citati requisiti di autonomia e indipendenza, comportando un'intollerabile coincidenza tra Soggetto controllore e controllato.

b) **Natura interna all'Ente**: come si ricava dall'art. 6 del D.Lgs. 231/01, le funzioni di vigilanza rimesse all'Organismo non possono essere integralmente affidate all'esterno, neppure attraverso dinamiche di *outsourcing*. Ciò, però, non significa, come di seguito precisato, che non possa farsi ricorso a consulenti esterni, la cui presenza garantisce l'autonomia e l'indipendenza dal Vertice Aziendale.

c) **Professionalità**: l'Organismo deve essere dotato di adeguati poteri e di competenze professionali appropriate al fine di garantire uno svolgimento efficace dei compiti di vigilanza previsti dal D.Lgs. 231/01. Ciò comporta, in caso di organo di controllo di natura collegiale, la scelta di membri aventi le conoscenze e le professionalità richieste per l'espletamento delle funzioni, quali la conoscenza della struttura interna dell'Ente, le competenze in materie aziendalistiche, organizzative e quelle prettamente giuridico-penalistiche. Tale necessaria professionalità, sempre nel caso di organismo di controllo di natura collegiale, può essere realizzata anche attraverso il ricorso ad uno o più consulenti esterni.

d) **Continuità di azione**: la costante attività di vigilanza e controllo richiesta dal D.Lgs. 231/01 impone che l'organismo in questione sia in grado di garantire una sufficiente continuità della sua azione. Ciò significa, pertanto, che tale organismo deve garantire una continua operatività, e, ove necessario, una costante presenza nell'azienda.

Possono essere nominati membri dell'OdV i Soggetti in possesso delle professionalità necessarie per l'espletamento delle funzioni e/o che abbiano maturato specifica esperienza in ambito aziendale. In particolare, le competenze richieste afferiscono alle materie giuridiche, economiche, finanziarie e alle scienze organizzative e aziendalistiche.

I membri dell'Organismo possono ricoprire funzioni o cariche in ambito aziendale, purché queste non comportino a titolo individuale poteri gestionali operativi incompatibili con l'esercizio delle funzioni dell'Organismo.

Costituiscono cause d'ineleggibilità dei componenti dell'OdV:

- la condanna, anche in primo grado, o l'applicazione della pena su richiesta ex artt. 444 e ss. c.p.p. per uno dei reati previsti dal D.Lgs. 231/2001;
- la condanna, anche in primo grado, a pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;
- la condanna anche in primo grado o l'applicazione della pena su richiesta ex artt. 444 e ss. c.p.p. per reati contro la pubblica amministrazione, per reati finanziari, o per reati che comunque incidano sull'affidabilità morale e professionale del Soggetto;
- la condizione giuridica di interdetto, inabilitato o fallito;
- l'esercizio o il potenziale esercizio di attività in concorrenza o in conflitto di interessi con quella svolta dalla Società.

I membri dell'Organismo di Vigilanza devono dichiarare, sotto la propria responsabilità, di non trovarsi in alcuna delle situazioni d'ineleggibilità o in altra situazione di conflitto d'interessi, con riguardo alle funzioni/compiti dell'Organismo di Vigilanza, impegnandosi, per il caso in cui si verificasse una delle predette situazioni (e fermo restando in tale evenienza l'assoluto e inderogabile obbligo di astensione), a darne immediata comunicazione al Consiglio di Amministrazione, onde consentire la sostituzione nell'incarico.

Costituiscono cause di decadenza dei componenti dell'OdV:

- la condanna in secondo grado o l'applicazione della pena su richiesta ex artt.444 e ss. c.p.p. per uno dei reati previsti dal D.Lgs. 231/2001;
- la condanna in secondo grado a pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;
- la condanna in secondo grado o l'applicazione della pena su richiesta ex artt.444 e ss. c.p.p. per reati contro la pubblica amministrazione, per reati finanziari, o per reati che comunque incidano sull'affidabilità morale e professionale del Soggetto;
- la condizione giuridica di interdetto, inabilitato o fallito;
- l'esercizio o il potenziale esercizio di attività in concorrenza o in conflitto di interessi con quella svolta dalla Società ;
- l'omessa comunicazione di una situazione di incompatibilità o di conflitto di interessi con riguardo alle funzioni/compiti dell'Organismo di Vigilanza o la violazione, in tali ipotesi dell'obbligo di astensione.

1.5.3 Durata in carica e cessazione

All'atto della nomina dei Componenti l'Organismo di Vigilanza, il CdA di Engineering D.HUB ha stabilito che gli Stessi restano in carica fino a loro revoca, deliberata dallo stesso CdA.

La cessazione dalla carica dei componenti dell'OdV è determinata - oltre che dalla revoca - da rinuncia, decadenza, impedimento permanente e, per quanto riguarda i membri interni alla Società nominati in ragione della funzione aziendale ricoperta, dal venir meno della titolarità di tale funzione.

La rinuncia da parte dei membri dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione per iscritto, unitamente alle motivazioni che l'hanno determinata. La rinuncia ha effetto immediato, se rimane in carica la maggioranza dei membri dell'Organismo o, in caso contrario, dal momento in cui la maggioranza dell'Organismo si è ricostituita, in seguito all'accettazione dei nuovi membri.

La revoca dell'incarico conferito a uno o più membri dell'Organismo di Vigilanza può essere deliberata dal Consiglio di Amministrazione, sentito il parere non vincolante del *Collegio Sindacale*, per giusta causa.

Per giusta causa di revoca deve intendersi:

- un grave inadempimento ai propri doveri/funzioni, così come definiti nel Modello;
- la condanna della Società, ai sensi del Decreto, anche con provvedimento non ancora passato in giudicato, motivato sulla base della "omessa o insufficiente vigilanza" da parte dell'Organismo;
- il verificarsi di una delle cause di decadenza;
- la violazione del divieto di comunicazione e diffusione delle informazioni.

In caso di cessazione per qualunque causa di un membro dell'Organismo, il Consiglio di Amministrazione provvede senza ritardo alla sua sostituzione con un'apposita delibera. In tal caso, il componente sostituto dura in carica fino alla scadenza degli altri membri dell'OdV.

In caso di cessazione del Presidente, le relative funzioni sono assunte, fino all'accettazione del nuovo Presidente, dal membro più anziano.

L'OdV e ciascuno dei suoi membri, nonché coloro dei quali l'OdV si avvarrà per l'espletamento delle proprie funzioni (siano questi Soggetti interni che esterni alla Società), non potranno subire conseguenze ritorsive di alcun tipo per effetto dell'attività svolta.

1.5.4 Convocazione, voto e delibere

Le riunioni dell'OdV sono convocate dal Presidente, ovvero su richiesta congiunta degli altri membri e sono valide con la presenza della maggioranza dei membri.

Le delibere dell'Organismo sono adottate a maggioranza assoluta e motivate con espressa indicazione dell'eventuale posizione minoritaria.

È fatto obbligo a ciascun membro dell'Organismo di dare notizia agli altri membri di ogni interesse in conflitto, per conto proprio o di terzi, con un'attività dell'Organismo, precisandone in particolare la natura, i termini, l'origine e la portata, astenendosi in ogni caso dal partecipare alle deliberazioni riguardanti l'attività stessa. Nel caso in cui al membro sia stata delegata un'attività, lo stesso deve astenersi dal compierla e investire della questione l'intero Organismo.

1.5.5 Conservazione delle informazioni e divieto di comunicare

Presso la Segreteria tecnica dell'Organismo è conservata, per un periodo minimo di dieci anni, copia cartacea e/o informatica di tutto il materiale relativo all'attività svolta.

A tal fine, la Società dota l'Organismo di strutture idonee alla conservazione del materiale su indicato.

L'accesso all'archivio da parte di Soggetti terzi deve essere preventivamente autorizzato dall'Organismo e svolgersi secondo modalità dallo stesso stabilite.

Su nomina del Titolare del trattamento, i membri dell'Organismo assumono, per quanto attiene alla gestione della casella e-mail e degli archivi cartaceo e informatico, la qualifica di Responsabili del trattamento dei dati personali ai sensi del, Regolamento Europeo n. 2016/679 e adottano ogni cautela idonea a preservare i dati stessi, garantendo un backup dei dati con cadenza trimestrale.

I Componenti dell'OdV, i Componenti delle strutture aziendali e i Consulenti di cui esso dovesse avvalersi, non possono comunicare o diffondere notizie, informazioni, dati, atti e documenti acquisiti nell'esercizio delle proprie attività, fatti salvi gli obblighi di comunicazione previsti dal *Modello* e dalle disposizioni vigenti.

1.5.6 Regolamento dell'OdV e relazioni al Vertice aziendale

L'Organismo di Vigilanza approva un proprio regolamento che ne disciplina il funzionamento.

L'Organismo di Vigilanza riporta i risultati della propria attività in un rapporto scritto semestrale trasmesso all'Amministratore Delegato. L'OdV trasmette inoltre un rapporto annuale al Collegio Sindacale.

L'Organismo di Vigilanza per l'esecuzione di specifiche attività di controllo si avvale della funzione di *Internal Auditing*, la quale, ad inizio anno, predispone il piano annuale degli interventi interni all'Azienda.

1.5.7 Funzioni e poteri dell'OdV

In conformità a quanto previsto dal D.Lgs. 231/01, all'Organismo di Vigilanza sono affidate le seguenti funzioni:

a) vigilare sulla reale efficacia ed effettività del *Modello di organizzazione e gestione*, relativamente alla prevenzione dei reati richiamati dal D.Lgs. 231/01;

b) vigilare sul rispetto del *Modello di organizzazione e gestione* e del *Codice etico*;

c) vigilare sulla continua adeguatezza del *Modello di organizzazione e gestione* relativamente alla eventuale intervenuta modifica della struttura aziendale e/o del quadro normativo e curarne l'eventuale aggiornamento.

Per l'effettivo ed efficace svolgimento delle predette funzioni, e in conformità a quanto previsto dall'articolo 6, comma 1, lett. b), del D.Lgs. 231/01, all'Organismo di Vigilanza sono riconosciuti i seguenti poteri:

- emanare le disposizioni ritenute necessarie per le attività di vigilanza e controllo, nonché per l'attivazione dei canali informativi di cui ai successivi paragrafi;
- raccogliere e conservare ogni informazione e/o notizia ritenuta utile e rilevante ai fini del decreto in oggetto;

- effettuare, eventualmente anche secondo metodi a campione, ogni opportuna verifica o indagine su operazioni, atti o condotte poste in essere all'interno della Società;
- ricorrere a consulenti esterni di comprovata professionalità;
- elaborare le informazioni e le notizie raccolte, quelle ugualmente pervenute attraverso i canali informativi di cui ai successivi paragrafi, nonché i risultati delle indagini e delle verifiche condotte;
- elaborare le proposte di modifica, aggiornamento e/o implementazione del Modello di organizzazione e gestione e del Codice Etico che dovessero risultare opportune;
- compiere quanto ritenuto opportuno per la diffusione della conoscenza del Modello di organizzazione e gestione all'interno della Società, nonché tra i Soggetti esterni (Collaboratori esterni, Fornitori e Partner) che dovessero entrare in contatto con la Società;
- comunicare per iscritto, al Consiglio di Amministrazione e al Collegio Sindacale la rilevazione di violazioni del *Modello*;
- elaborare, in coordinamento con la Direzione Generale *Human Resource & Organization*, adeguati metodi per la formazione del personale relativamente al decreto in oggetto (ferma restando la competenza esclusiva della Direzione Generale *Human Resource & Organization* per la concreta attuazione degli elaborati metodi);
- elaborare, in coordinamento con le Direzioni di Business e la Direzione Generale Amministrazione Finanza e Controllo, le adeguate clausole contrattuali per una migliore regolamentazione, ai sensi del decreto in oggetto, dei rapporti con Soggetti terzi (ferma restando la competenza esclusiva delle Direzioni di Business e della Direzione Generale Amministrazione Finanza e Controllo per la concreta attuazione delle elaborate clausole contrattuali);
- accedere liberamente alla documentazione utile per le finalità istituzionali dell'Organismo di Vigilanza in possesso delle diverse Direzioni aziendali, degli Amministratori e del Collegio Sindacale;
- ricevere periodicamente dai Soggetti indicati nel presente Modello le informazioni indicate nel paragrafo "*Flussi informativi*"
- promuovere, ferma la competenza del vertice aziendale per l'irrogazione delle sanzioni e del relativo procedimento disciplinare, l'applicazione di eventuali sanzioni disciplinari, anche nel caso di omesso invio all'OdV dei *Flussi informativi* richiesti;
- coordinare il monitoraggio delle attività in relazione ai princìpi stabiliti dal *Modello*, anche con il supporto delle diverse funzioni aziendali indicendo, quando opportuno, apposite riunioni.

Allo scopo di consentirgli di svolgere concretamente le proprie funzioni e di esercitare efficacemente i propri poteri, nel rispetto delle prerogative di *autonomia* e *indipendenza* che lo caratterizzano, all'OdV è assegnato dal CdA un budget di spesa *congruo*, volto ad assicurare un corretto svolgimento dei propri compiti (es. consulenze specialistiche, trasferte, ecc.).

1.5.8 Obblighi d'informativa

L'Organismo di Vigilanza è destinatario dei flussi informativi relativi all'attuazione del *Modello di organizzazione e gestione* e del *Codice Etico*, secondo i canali di informazione attivati in conformità a quanto previsto dall'articolo 6, comma 2, lett. d), del D.Lgs. 231/01.

I Dipendenti della Società ed, in particolare, i "*Responsabili interni della fornitura dei flussi informativi ex D.Lgs. 231/01*" individuati all'interno dell'Azienda (di seguito, per brevità: "*Responsabili flussi informativi 231*") hanno l'obbligo di trasmettere all'Organismo di Vigilanza quanto segue:

- i provvedimenti e/o le notizie provenienti dalla Pubblica Amministrazione dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti (cfr. articolo 8 del D.Lgs. 231/01), per uno o più dei reati previsti dal medesimo decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti relativamente ad un procedimento giudiziario per uno o più dei reati previsti dal D.Lgs. 231/01;
- i rapporti redatti dai Responsabili di ogni Direzione aziendale, dai quali possano emergere fatti, atti e condotte, anche omissive, potenzialmente rilevanti ai sensi del D.Lgs. 231/01;

- le notizie relative all'instaurazione ed alla conclusione di procedimenti disciplinari, ivi comprese le sanzioni irrogate ed i provvedimenti di archiviazione, relativi alla violazione del *Modello di organizzazione e gestione*.

Inoltre, al fine di garantire un corretto esercizio delle proprie funzioni, l'Organismo di Vigilanza deve essere informato, da chiunque ne abbia contezza, di ogni notizia attinente:

- all'attuazione del *Modello* all'interno della Società, anche con riferimento all'applicazione dei protocolli;
- all'eventuale esistenza di aree di attività prive del tutto o in parte di regolamentazione;
- alle eventuali lacune del sistema;
- all'individuazione di potenziali anomalie nell'applicazione del *Modello*;
- alle proposte di integrazione e le modifiche da apportare alle procedure operative o al *Modello* stesso;
- alle violazioni o sospette violazioni del *Modello*, delle procedure ivi richiamate e del *Codice Etico*;
- al compimento di operazioni straordinarie da parte della Società
- alla commissione di reati all'interno dell'Azienda.

Tutte le comunicazioni inviate all'*Organismo di Vigilanza* della Società devono avere forma scritta e possono essere inoltrate, eventualmente in modo anonimo, tramite e-mail, all'indirizzo **231@eng.it** messo a disposizione dall'Organismo.

La suddetta casella di posta elettronica è accessibile ai Componenti dell'OdV ed al Responsabile dell'*Internal Auditing* ed è resa inaccessibile a Terzi.

L'Organismo di Vigilanza farà in modo che i Soggetti segnalanti siano tutelati contro ogni forma di ritorsione, discriminazione e/o penalizzazione, garantendo, nei limiti degli obblighi di legge e della tutela dei diritti della Società, l'anonimato dei medesimi segnalanti e la riservatezza di quanto segnalato.

1.5.9 Flussi informativi verso l'OdV

La Direzione Processi e Audit Interno, in persona del Direttore, o di Soggetto dallo stesso individuato, comunica in forma sintetica all'Organismo di Vigilanza le verifiche effettuate nell'ambito della Società e i relativi esiti.

Inoltre, precisato che la Società attribuisce, d'ufficio, il ruolo di "*Responsabile flussi informativi 231*" ai Responsabili delle Direzioni Generali e delle Direzioni Centrali di Gruppo, i *Responsabili flussi informativi 231* inviano all'Organismo di Vigilanza:

1) con cadenza quadrimestrale:
   - informazioni (di tipologia specificamente individuata) ritenute utili alla tempestiva identificazione di attività *a rischio* (in ottica D.Lgs. 231/01) ovvero utili a documentare la corretta applicazione delle prescrizioni contenute nel presente *Modello*;
   - ogni altro dato ritenuto utile per una migliore attuazione del *Modello*;
2) a due mesi dalla scadenza del periodo quadrimestrale di cui al flusso precedente:
   - un'informativa sintetica di aggiornamento circa l'eventuale manifestarsi di fatti rilevanti e/o di inosservanze significative meritevoli di segnalazione;
3) di volta in volta, obbligatoriamente e immediatamente, i dati relativi:
   - alla commissione dei reati-presupposto e all'adozione di comportamenti non in linea con le regole di condotta previste dal *Modello*;
   - ai provvedimenti e/o alle notizie da cui si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, la cui commissione si assuma essere avvenuta nella Società; ovvero l'esistenza di un procedimento penale a carico della stessa Società;

- alle richieste di assistenza legale inoltrate dai Soggetti nei confronti dei quali la Magistratura proceda per i reati previsti dal Decreto;
- a ogni anomalia o atipicità riscontrata nell'ambito delle attività a rischio, alle notizie relative alle asserite o accertate violazioni del *Modello* o del *Codice Etico* e alle eventuali sanzioni disciplinari irrogate, ovvero ai provvedimenti di archiviazione di tali procedimenti, con le relative motivazioni.

I Collaboratori esterni, i Fornitori e i *Partner* effettuano le eventuali segnalazioni relative all'attività svolta per la Società direttamente all'Organismo di Vigilanza, con le modalità già precedentemente indicate.

L'Organismo di Vigilanza:

1) garantisce la riservatezza dell'identità del segnalante e delle persone oggetto della segnalazione; il segnalante è inoltre garantito contro qualsiasi forma di ritorsione, discriminazione o penalizzazione;
2) valuta le segnalazioni ricevute e, ove necessario, svolge un'attività istruttoria, senza obbligo di comunicare al segnalante la decisione assunta.

Ove ravvisi una violazione del *Modello*, l'Organismo di Vigilanza:

- promuove presso l'apposita Direzione un procedimento disciplinare a carico del Dipendente ritenuto responsabile;
- informa il Consiglio di Amministrazione e il Collegio Sindacale nel caso di violazione commessa da uno o più membri dei predetti Organi sociali;
- chiede alla Direzione di competenza di porre in esecuzione le clausole contrattuali di risoluzione e/o recesso dei rapporti con Collaboratori esterni, Fornitori e Partner, nel caso di violazione agli stessi addebitabile.

1.5.10 Le segnalazioni delle violazioni del Modello alla luce della normativa in materia di "whistleblowing"

Con l'approvazione della proposta di legge n. 3365-B ("*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*"), intervenuta il 18 ottobre 2017, è stata estesa al settore privato l'applicabilità della disciplina relativa al sistema di tutela del dipendente pubblico che segnala illeciti di cui sia venuto a conoscenza in ragione del proprio rapporto di lavoro, attraverso l'inserimento, nell'art. 6 del D. Lgs. 231/2001, dei commi 2 bis, ter e quater.

In forza del nuovo dettato normativo, sono oggetto di segnalazione:

(a) le condotte illecite rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti;

(b) le violazioni del Modello di organizzazione e gestione dell'ente, di cui i Destinatari siano venuti a conoscenza in ragione delle funzioni svolte.

I soggetti tenuti a trasmettere le predette segnalazioni, ai sensi dell'art. 6, comma 2-bis, lett. a) sono:

(i) "*le persone indicate nell'articolo 5, comma 1, lettera a)*" del Decreto e, cioè, coloro i quali rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che esercitano, anche di fatto, la gestione e il controllo dello stesso;

(ii) "*le persone indicate nell'articolo 5, comma 1, lettera b)*" del Decreto, ossia coloro i quali sono sottoposti alla direzione o alla vigilanza di uno dei soggetti indicati nella superiore lettera (i).

Le segnalazioni possono riguardare qualsiasi ambito aziendale rilevante ai fini dell'applicazione del Decreto e del Modello vigente e devono contenere:

- elementi utili alla ricostruzione del fatto segnalato, con allegazione, ove possibile, di relativa documentazione a supporto;
- informazioni che consentano, ove possibile, la identificazione del soggetto autore del fatto segnalato;

- l'indicazione delle circostanze in occasione delle quali si è venuti a conoscenza del fatto segnalato.

Il Decreto prescrive, inoltre, la definizione di uno o più canali che garantiscano "*la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione" (art. 6, comma 2-bis, lett. a), nonché "almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante*" (art. 6, comma 2-bis, lett. b).

In attuazione del dettato normativo, il Gruppo si è dotato di una applicazione informatica tramite la quale consente ai propri dipendenti la segnalazione circostanziata, e fondata su elementi di fatto precisi e concordanti, di condotte illecite o di violazioni del Modello di cui siano venuti a conoscenza in ragione delle funzioni svolte.

L'applicazione è basata sulla soluzione "GlobalLeaks", certificata ed utilizzata dall'Autorità Nazionale Anticorruzione (ANAC), e fa sì che le segnalazioni siano indirizzate all'Organismo di Vigilanza nominato ai sensi del D. Lgs. 231/01, con la garanzia della tutela della riservatezza circa l'identità del segnalante, in conformità a quanto previsto dall'articolo 2 della Legge 179/2017, per permettere di effettuare in sicurezza la segnalazione degli eventuali illeciti dei quali si sia venuti a conoscenza nello svolgimento della propria attività lavorativa.

Al fine di rendere consapevoli i destinatari del nuovo sistema di segnalazione, sui propri diritti e sulle modalità di funzionamento del sistema stesso, la Società ha predisposto la procedura "*PGP24_0_Normativa Whistleblowing-Segnalazione di reati o irregolarità*" resa disponibile sulla INTRANET aziendale, con specifica comunicazione.

È possibile accedere all'applicazione per effettuare le segnalazioni tramite il Portale Segnalazioni – Whistleblowing accessibile dal link: https://ewb.eng.it.

In alternativa è possibile effettuare le segnalazioni tramite l'indirizzo e-mail 231@eng.it.

In ultimo, le segnalazioni possono essere inviate a mezzo del servizio postale, con lettera recapitata presso la sede della Società, o tramite corrispondenza interna, intestata all'Organismo di Vigilanza c/o Piazzale dell'Agricoltura n. 24 – 00144 Roma; in tal caso, per poter usufruire della garanzia della riservatezza, è necessario che la segnalazione venga inserita in una busta chiusa che rechi all'esterno l'indicazione "riservata/personale".

L'OdV, destinatario e unico detentore delle segnalazioni ricevute, assicura la riservatezza delle informazioni acquisite e della identità del segnalante che è protetta in ogni contesto successivo alla segnalazione, ad eccezione dei casi in cui è configurabile una responsabilità penale o civile del soggetto segnalante e delle ipotesi in cui l'anonimato non è opponibile per legge, (a titolo esemplificativo, indagini penali, tributarie o amministrative, ispezioni di organi di controllo, etc.).

L'OdV valuta la rilevanza ai sensi del D. Lgs. n. 231/01 delle segnalazioni ricevute, ponendo in essere ogni attività ritenuta necessaria a tal fine e, avvalendosi, se necessario, della collaborazione delle strutture aziendali competenti. Qualora la segnalazione risultasse fondata, in tutto o in parte, l'OdV trasmetterà all'Organo Amministrativo o alla competente struttura/Funzione aziendale, l'esito delle verifiche condotte per le conseguenti determinazioni anche in ordine ad eventuali procedimenti disciplinari.

L'Organismo custodisce per un periodo minimo di 10 anni copia cartacea e/o informatica delle segnalazioni ricevute.

La Società garantisce la tutela di qualunque soggetto segnalante contro ogni forma di ritorsione, discriminazione o penalizzazione, secondo quanto disposto dall'art. 6, comma 2-bis, lett. c) del Decreto.

La Società si astiene, quindi, dal porre in essere "*atti di ritorsione o discriminatori diretti o indiretti, nei confronti del segnalante*" (quali, a titolo esemplificativo, il licenziamento, il mutamento di mansioni, trasferimenti, sottoposizione del segnalante a misure organizzative aventi effetti negativi sulle condizioni di lavoro) "*per motivi collegati, direttamente o indirettamente, alla segnalazione*".

1.5.11 Risposta alla notizia di reato

Qualora venga a conoscenza, attraverso qualunque canale informativo, di una *notizia di reato* ex D.Lgs. 231/01 commesso all'interno dell'organizzazione aziendale, l'Organismo di Vigilanza attiva una serie di iniziative volte a rilevare i *punti di debolezza* del *Modello* eventualmente sfruttati nella commissione del reato stesso.

A tal fine, anche usufruendo del supporto del Servizio di Internal Auditing, vengono individuati ed intervistati i Soggetti coinvolti, in vario ruolo, o informati dei fatti che hanno determinato il concretizzarsi del reato, vengono ricostruite le fasi dei processi aziendali interessati, analizzati i controlli prescritti dai protocolli, sia quelli attuati (e relative evidenze), che quelli eventualmente omessi.

Laddove, a seguito di una segnalazione anonima, le indagini dovessero focalizzarsi sul comportamento di un Dipendente, lo stesso verrà informato della cosa da parte di un Responsabile incaricato dall'OdV, a garanzia di un comportamento trasparente da parte dell'Azienda ed allo scopo di fugare sospetti di un atteggiamento aziendale pregiudizialmente colpevolistico nei confronti del Dipendente.

Ottenuto un quadro sufficientemente chiaro di quanto accaduto e valutate, nel merito, le circostanze emerse, l'OdV procederà, di volta in volta, adottando una o più delle seguenti iniziative:

- informerà i Vertici Aziendali dell'accaduto, in particolare la *Direzione Generale Human Resource & Organization*, alla quale proporrà, se del caso, l'applicazione di appropriate sanzioni disciplinari;
- informerà gli altri organi di controllo aziendali per le loro eventuali autonome iniziative;
- solleciterà l'introduzione nel *Modello* di specifici protocolli (o, eventualmente, la modifica di quelli esistenti) al fine di meglio garantire rispetto al rischio del ripetersi di quanto accaduto;
- proporrà alla *Direzione Generale Human Resource & Organization* specifici adeguamenti degli interventi formativi normalmente svolti in Azienda, adeguamenti focalizzati sul rischio di commissione del reato in questione, così come potrà proporre a detta Direzione la previsione di sanzioni disciplinari più severe.

1.5.12 Nomina e composizione

In data 04/08/2014 il Consiglio di Amministrazione di Engineering D.HUB ha deliberato la nomina dei Componenti l'*Organismo di Vigilanza* ex D.Lgs. 231/01.

Ciascun componente è in possesso dei richiesti requisiti di autonomia, indipendenza, onorabilità, professionalità e continuità d'azione, nonché delle competenze necessarie per lo svolgimento dei compiti assegnati.

1.6 Formazione e informazione del Personale e dei Contraenti esterni

Ai fini del buon funzionamento del *Modello di organizzazione e gestione* è necessario che tutti i suoi protocolli, ovvero i principali documenti da esso richiamati, siano oggetto di una diffusione capillare, efficace ed autorevole.

È inoltre opportuno che tale processo di comunicazione sia accompagnato da un adeguato programma di formazione rivolto al personale delle aree a rischio, allo scopo di illustrare le ragioni di opportunità, a fianco a quelle giuridiche, che ispirano le regole e la loro portata concreta. Detto processo di formazione e informazione dei lavoratori deve avvenire mediante un sistema che preveda una comunicazione adeguata, chiara, dettagliata e periodicamente ripetuta.

- La Direzione Generale *Human Resource & Organization* valuta, sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, l'introduzione di nuovi e ulteriori criteri di selezione del personale che garantiscano in misura ancora maggiore la Società rispetto alla commissione di reati al proprio interno.
- La Direzione Generale *Human Resource & Organization* cura, sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, la formazione del personale relativamente al contenuto del D.Lgs. 231/01, del *Modello di organizzazione e gestione* e del *Codice Etico* della Società.

L'Organismo di Vigilanza promuove l'informazione e la formazione del personale sui contenuti del *Modello*, in collaborazione con la Direzione Generale Amministrazione Finanza e Controllo, coordinandosi con altre Direzioni Aziendali di volta in volta coinvolte nell'applicazione del *Modello*.

Quanto alla formazione del personale:

1) per i neo-assunti: al momento dell'assunzione viene fornito loro un documento di autoformazione sui contenuti del D.Lgs. 231/01;

2) per tutto il personale (Soggetti in posizione *apicale* e non):

   - ✓ ciascuna verifica condotta dalla funzione di Internal Auditing presso una determinata Unità Organizzativa prevede una specifica sessione formativa rivolta ai Referenti della stessa, finalizzata a richiamare l'importanza di un rigoroso rispetto dei princìpi e delle norme contenute nel *Codice Etico del Gruppo* e nel *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*, nonché a richiamare la tipologia di reati a cui l'Unità Organizzativa risulta particolarmente esposta, evidenziando eventuali nuovi reati-presupposto che fossero stati introdotti dal legislatore;
   - ✓ utilizzando un'apposita infrastruttura di e-learning, vengono erogati corsi di aggiornamento sui contenuti del *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*; tali corsi sono destinati, prevalentemente, a Capi Progetto ed a Responsabili di Centri di Produzione; vengono, inoltre, organizzate delle sessioni di formazione con incontri frontali in aula;
   - ✓ l'adozione del *Modello* e, successivamente, dei suoi aggiornamenti, è comunicata a tutte le Risorse presenti in Azienda, previa pubblicazione della nuova versione all'interno della rete intranet aziendale, con l'invio di una e-mail illustrativa ed esplicativa.

Le Direzioni Generali ed, in particolare, la Direzione Generale Amministrazione Finanza e Controllo potranno, sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, introdurre nuovi ed ulteriori criteri di selezione dei terzi contraenti con la Società (Collaboratori esterni, Fornitori, Partner, etc.) che garantiscano in misura ancora maggiore la Società rispetto alla commissione di reati.

Le citate Direzioni Generali curano, anche sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, l'informativa ai terzi contraenti con la Società (Collaboratori esterni, Fornitori, Partner, etc.) relativamente al Decreto Legislativo 231/2001 ed alle misure di prevenzione adottate dalla Società.

I Collaboratori esterni, i Fornitori e i Partner vengono informati, mediante specifiche clausole contrattuali, del loro obbligo di rispettare i princìpi contenuti nel *Codice Etico Engineering*, nonché del loro obbligo di non commettere reati di cui al D.Lgs. 231/01, pena il profilarsi di responsabilità a livello contrattuale.

1.7 Il Sistema disciplinare

1.7.1 Introduzione

Ai sensi dell'articolo 6, comma 2, lett. e), del D.Lgs. 231/01, il *Modello di organizzazione e gestione* deve prevedere un idoneo sistema disciplinare in grado di sanzionare il mancato rispetto del *Modello* stesso.

Si tratta di un elemento imprescindibile, in assenza del quale difficilmente potrebbe operare con pieno effetto, a favore della Società, il c.d. "scudo protettivo" contro le conseguenze previste dal D.Lgs. 231/01.

Un siffatto apparato sanzionatorio deve essere efficace, ma al tempo stesso pienamente conforme alla disciplina giuslavoristica vigente nel nostro ordinamento (in particolare: articoli 2104 e ss. del codice civile; articolo 7 della legge n. 300/1970; articoli 23 e ss. del Contratto Collettivo Nazionale di Lavoro).

- A tale scopo, in conformità a quanto prescritto dall'articolo 7 della legge n. 300/1970 (c.d. Statuto dei Lavoratori) la Direzione Generale *Human Resource & Organization*, in coordinamento con l'Organismo di Vigilanza, provvede ad assicurare la piena conoscenza del Modello di organizzazione e gestione, anche attraverso la pubblicazione sul sito della Capogruppo .In ossequio alla citata prescrizione contenuta nella L. 300/70, l'Azienda provvede, infatti, a pubblicare nel portale internet del Gruppo, **www.eng.it**, alla sezione "Investor Relations - Corporate Governance – *Documenti e modelli societari*", il *Codice Etico* ed a pubblicare nella intranet aziendale il *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*.

L'applicazione delle sanzioni disciplinari è indipendente e autonoma rispetto all'esito di un eventuale procedimento penale.

Il sistema disciplinare, ai sensi dell'art. 6, comma 2 bis, lett. d) del Decreto, sanziona altresì la violazione delle misure poste a tutela di chi abbia effettuato una segnalazione secondo il sistema "Whistleblowing", nonché l'effettuazione, con dolo o colpa grave, di segnalazioni che si rivelano infondate.

1.7.2 Il sistema sanzionatorio per il Personale non dirigente

Per i *Dipendenti* l'osservanza delle norme del *Codice Etico* e del *Modello di Organizzazione e Gestione ex D.Lgs. 231/01* deve considerarsi parte essenziale degli obblighi contrattuali dagli stessi assunti ai sensi e per gli effetti dell'art. 2104 del Codice Civile; pertanto, i comportamenti tenuti in violazione del *Codice Etico* o del *Modello di Organizzazione e Gestione 231/01* sono considerati inadempimento degli obblighi primari del rapporto di lavoro ed hanno rilevanza disciplinare. Il procedimento disciplinare, l'irrogazione della sanzione, l'esecuzione, la contestazione e l'impugnazione della stessa sono disciplinati in conformità a quanto previsto dallo Statuto dei Lavoratori e dal Contratto Collettivo Nazionale di Lavoro.

In particolare:

1) il datore di lavoro non può adottare nessun provvedimento disciplinare nei confronti del lavoratore senza avergli prima contestato l'addebito e senza averlo sentito a sua difesa;
2) salvo che per il richiamo verbale, la contestazione deve essere effettuata per iscritto ed i provvedimenti disciplinari non possono essere comminati prima che siano trascorsi 5 (cinque) giorni, nel corso dei quali il lavoratore può presentare le sue giustificazioni;
3) se il provvedimento non viene comminato entro 6 (sei) giorni successivi a tali giustificazioni, queste ultime si ritengono accolte;
4) il lavoratore può presentare le proprie giustificazioni anche verbalmente, con l'eventuale assistenza di un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato;
5) la comminazione del provvedimento disciplinare deve essere motivata e comunicata per iscritto;
6) ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei 20 (venti) giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. In tal caso, la sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio;
7) qualora il datore di lavoro non provveda, entro 10 (dieci) giorni dall'invito rivoltogli dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto;
8) se il lavoratore adisce l'autorità giudiziaria, la sanzione disciplinare resta sospesa fino alla definizione del giudizio;
9) il licenziamento per mancanze può essere impugnato dal lavoratore secondo le procedure previste dall'articolo 7 della legge 604/1966, così come confermato dall'articolo 18 dello Statuto dei Lavoratori. Pertanto, il licenziamento per mancanze può essere impugnato, dinanzi al tribunale in funzione di giudice del lavoro, a pena di decadenza entro 60 (sessanta) giorni dalla ricezione della sua comunicazione;
10) non si può tenere conto ad alcun effetto delle sanzioni disciplinari decorsi 2 (due) anni dalla loro applicazione.

- In coerenza con le richiamate regolamentazioni legislative e contrattuali, l'inosservanza delle norme del *Codice Etico* e del *Modello di Organizzazione e Gestione ex D.Lgs. 231/01* espone il Personale a sanzioni disciplinari che saranno decise ed applicate dalla *Direzione Generale Human Resource & Organization* dell'Azienda, che ne valuterà tipologia ed entità tenendo conto:
  - dell'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia evidenziata;

- del comportamento complessivo del Dipendente, con particolare riguardo alla sussistenza o meno di precedenti sanzioni disciplinari;
- della posizione funzionale e delle mansioni del Dipendente coinvolto;
- di eventuali altre circostanze collegate alla violazione, in particolare del fatto che essa attenga a reati "*di particolare rilevanza*", fra i quali vengono ricompresi, oltre ai reati inerenti la mancata tutela della salute e della sicurezza sul lavoro, anche i seguenti (in virtù della tipologia delle attività svolte in Azienda):
  - ✓ reati inerenti i rapporti con la P.A.,
  - ✓ reati informatici.

A tal proposito, le seguenti possono essere considerate indicazioni a cui far riferimento (da valutare nell'ordine con cui vengono esposte):

- si considera applicabile il richiamo verbale nei casi in cui siano tutte vere le seguenti circostanze:
  - ✓ non risulta evidente l'intenzionalità del comportamento o lo stesso evidenzia un grado lieve di negligenza, imprudenza o imperizia;
  - ✓ nel passato al Responsabile del comportamento sanzionato non furono mai comminati provvedimenti disciplinari per reati ex D.Lgs 231/01;
  - ✓ il comportamento non attiene a reati "*di particolare rilevanza*" (come sopra identificati);
- si considera applicabile una sanzione non più lieve del *licenziamento con preavviso* nei casi in cui siano tutte vere le seguenti circostanze:
  - ✓ risulta evidente l'intenzionalità del comportamento e lo stesso evidenzia un grado elevato di negligenza, imprudenza o imperizia;
  - ✓ nel passato al Responsabile del comportamento sanzionato furono già comminati provvedimenti disciplinari, diversi dal richiamo verbale, per reati ex D.Lgs 231/01;
  - ✓ il comportamento attiene a reati "di particolare rilevanza"
- si considera applicabile una sanzione non più lieve dell'ammonizione scritta e/o della multa e/o della *sospensione* nei casi che non rientrano nelle casistiche sopra descritte.

È compito dell'Organismo di Vigilanza monitorare il sistema sanzionatorio contenuto nel *Modello di organizzazione e gestione*, nonché elaborare le eventuali proposte di modifica da inoltrare al Consiglio di Amministrazione.

1.7.3 Il sistema sanzionatorio per il Personale dirigente

Qualora i Dirigenti della Società si rendessero responsabili di violazioni delle norme e delle prescrizioni contenute nel *Codice Etico* o nel *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*, ovvero nel caso in cui avessero violato lo specifico obbligo di vigilanza sui sottoposti, saranno applicabili nei confronti dei medesimi Dirigenti le misure più idonee, in conformità a quanto previsto dalla legge e dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti Industriali, nel rispetto del criterio di proporzionalità di cui all'art. 2106 del codice civile.

1.7.4 Altre misure di tutela

Qualora gli Amministratori o i Sindaci della Società si rendessero responsabili di violazione delle procedure previste dal *Modello di organizzazione e gestione* o dell'adozione di un comportamento non conforme a quanto prescritto dal medesimo *Modello* o dal *Codice Etico del Gruppo*, l'Organismo di Vigilanza informerà senza indugio il Consiglio di Amministrazione e il Collegio Sindacale affinché sia adottato ogni provvedimento ritenuto opportuno e previsto dalla vigente normativa.

A fronte di specifiche clausole presenti all'interno dei contratti stipulati dalla Società con Soggetti terzi (Collaboratori esterni, Fornitori, Partner, etc.), l'eventuale violazione da parte di questi ultimi di quanto previsto dal *Modello di organizzazione e gestione* della Società potrà comportare le conseguenze previste dalle medesime clausole, ivi comprese, a titolo esemplificativo, la risoluzione, il recesso e il risarcimento dei danni.

2 SEZIONE SPECIALE

2.1 Premessa

Nella presente sezione vengono illustrati i reati-presupposto ricompresi nel perimetro del D.Lgs. 231/01 esclusi quelli non ritenuti concretamente realizzabili nel contesto aziendale. Per ciascuna tipologia di reato:

- viene descritta la fattispecie di riferimento;
- ne viene fornita una contestualizzazione aziendale, dove la descrizione della "*modalità di commissione"* del reato-presupposto scaturisce dall'analisi effettuata del rischio di effettiva commissione del reato;
- vengono descritti sinteticamente norme di comportamento, protocolli e controlli applicati in Azienda a presidio del rischio di commissione del reato-presupposto a cui ci si riferisce, così come vengono forniti i nomi dei documenti aziendali di riferimento. Ciascuna descrizione viene identificata dal codice "*Id. Protoc.*".

Relativamente a quest'ultimo punto, come già anticipato in altro contesto, per ciascun "*Id. Protoc.*" citato nel Modello, i protocolli e i controlli di dettaglio prescritti in Azienda sono accessibili, oltre che consultando le Procedure puntualmente referenziate, anche consultando uno specifico documento (ad uso interno) che li elenca.

La sequenza logica adottata, nei successivi paragrafi, per la trattazione dei vari reati è coerente con la sequenza degli articoli del D.Lgs. 231/01 che richiamano i reati-presupposto.

Verranno poi trattati i cosiddetti "*reati transnazionali*", non fisicamente *compresi* nel D.Lgs. 231/01, ma introdotti dalla Legge n. 146/2006 che riconosce, per i reati richiamati, la *responsabilità amministrativa degli Enti*, facendo riferimento, per le sanzioni da applicare, a specifici articoli del D.Lgs. 231/01.

Infine, ci si soffermerà brevemente sull'art. 23 del Decreto rubricato "*Inosservanza delle sanzioni interdittive*" che sanziona la trasgressione degli obblighi e/o dei divieti inerenti alle sanzioni o alle misure cautelari interdittive irrogate nei confronti dell'ente.

2.2 Principi generali di comportamento

- Con riferimento ai reati-presupposto qui considerati, devono anzitutto essere rispettati, come indicazioni cogenti, i principi, i valori e le norme contenuti nel Codice Etico del Gruppo Engineering, da considerare, a ogni effetto, parte integrante del Modello di Organizzazione e Gestione ex D.Lgs. 231/01; entrambi devono essere pubblicati nella rete intranet aziendale e, per quanto riguarda il Codice Etico, nel portale del Gruppo (www.eng.it). Il loro contenuto deve essere oggetto di formazione rivolta ai Dipendenti.
- È comunque assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di uno dei reati qui considerati.
- È indispensabile che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza.
- È indispensabile che sia garantito il rispetto della normativa vigente, nonché delle procedure e dei protocolli aziendali, sia relativi al Ciclo attivo che a quello passivo, nonché quelli in materia di gestione ed impiego delle risorse e dei beni aziendali, in particolare per quelli di provenienza estera.

- È indispensabile che sia mantenuto un contegno chiaro, trasparente, diligente e collaborativo con le Pubbliche Autorità, con particolare riguardo alle Autorità Giudicanti e Inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste.
- Chiunque in Azienda venga a conoscenza di comportamenti tenuti da Dipendenti/Collaboratori che integrano uno dei reati-presupposto considerati nel presente documento è tenuto ad informare il proprio Responsabile diretto, la Direzione Processi e Audit Interno e l'Organismo di Vigilanza.

2.3 Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (Art. 24 del D.Lgs. 231/01)

2.3.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 24 del Decreto richiama specificatamente i seguenti reati.

- Malversazione a danno dello Stato o di altro ente pubblico
- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee;
- Truffa in danno dello Stato o di altro ente pubblico
- Truffa aggravata per il conseguimento di erogazioni da parte dello Stato, di enti pubblici o delle Comunità europee
- Frode informatica in danno dello Stato o di altro ente pubblico

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

- Destinazione di contributi, di sovvenzioni o di finanziamenti a fini diversi da quelli fissati dall'Ente pubblico che li ha concessi
- Fornitura di false informazioni o omissioni di informazioni dovute (ad es.: in sede di Offerta/ Risposta a bando di gara) allo scopo di ottenere indebitamente da un Ente pubblico, contributi, finanziamenti, decontribuzioni o analoghi benefici
- Mediante artifici o raggiri, inducendo taluno in errore, ci si procura, a danno dello Stato o di altro Ente pubblico, un ingiusto profitto, contributi, finanziamenti o analoghi benefici
- In danno dello Stato o di altro ente pubblico, procurando all'Azienda o ad altri un ingiusto profitto, si altera il funzionamento di un sistema informatico/telematico o si interviene senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti in un sistema informatico o ad esso pertinenti.

2.3.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Dir. Gen. P.A. e Sanità
- Dir. Gen. Tecnica Innovazione e Ricerca
- Scuola di IT & Management "ENRICO DELLA VALLE"
- Infatti tali UU.OO. si rivolgono a settori di mercato perfettamente identificabili con i Soggetti richiamati da questo articolo del Decreto: Stato, Enti Pubblici e Istituzioni comunitarie. La Scuola di IT & Management "ENRICO DELLA VALLE" e la Dir. Gen. Tecnica Innovazione e Ricerca, in particolare, potrebbero essere destinatarie di finanziamenti, sovvenzioni o contributi erogati dall'Ente Pubblico.

In misura minore possono risultare sensibili le seguenti UU.OO.:

- Dir. Gen. Human Resource & Organization (assunzione di personale a fronte di finanziamenti/decontribuzioni)
- Dir. Gen. Amm. Fin. e Controllo (i cui uffici potrebbero agevolare il perfezionamento del reato).

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Partecipazione ad una gara: attività preliminari alla formalizzazione della Risposta al bando; formalizzazione della Risposta
- Gestione subappalti: acquisizione autorizzazione dal Cliente
- Erogazione di forniture (es.: corsi di formazione) che godono di finanziamenti o rimborsi da parte di Enti Pubblici
- Project Management/Analisi-Revisione Offerta o Contratto
- Project Management/Assegnazione responsabilità Capo Progetto e formazione Gruppo di Lavoro
- Project Management/Gestione rapporti verso Cliente, Fornitori o eventuali Partner in RTI/ATI
- Project Management/Controllo e verifica, in corso d'opera, del rispetto dei requisiti contrattuali
- Project Management/Rendicontazione all'Ente finanziatore dei costi sostenuti
- Ricerca e selezione diretta del Personale
- Agevolazioni finanziarie legate all'assunzione del Personale
- Gestione Amministrativa RTI-ATI/Gestione rapporti economici fra Partner
- Conferimento ed impiego di Procure

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- Allo scopo di facilitare l'assegnazione della commessa, la Risposta al bando di gara (o l'Offerta) viene predisposta in modo incompleto o non del tutto veritiero, facendo ricorso a imprecisioni, omissioni, falsità o analoghi artifici.
- I risultati dell'attività di definizione dei costi preventivati, di quelli sostenuti e degli Stati d'Avanzamento Lavori non scaturiscono da processi trasparenti e documentabili.
- Svolgimento di programmi formativi difformi, per oggetto, modalità o docenza, da quelli previsti nel progetto approvato dall'Ente erogatore
- Erogazione di corsi di formazione a discenti privi dei requisiti che erano stati indicati dall'Ente che concede contributi, sovvenzioni o finanziamenti
- Assunzione di Personale avente requisiti difformi da quelli che erano stati indicati dall'Ente che concede finanziamenti o decontribuzioni
- Attuazione di irregolari compensazioni economiche fra Partner di un RTI/ATI
- Nell'ambito dell'erogazione di una fornitura allo Stato, ad un Ente Pubblico o Comunitario, si interviene in modo illecito su informazioni e programmi pertinenti al suo Sistema Informativo.

Si segnala infine che l' Azienda ha deciso di connotare come reati "*di particolare rilevanza*" gli eventuali reati commessi nell'ambito dei rapporti (preliminari o successivi alla formalizzazione contrattuale) instaurati con una Pubblica Amministrazione, *Centrale* o *Locale*, o con Istituzioni Comunitarie e di sanzionarli con maggior severità nell'ambito del *sistema disciplinare* descritto nel presente Modello.

2.3.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.3.3.1 Principi specifici di comportamento

- Durante la fase che precede l'emissione di un bando di gara e in quella di partecipazione alla stessa, il personale di una Società del Gruppo Engineering che, con ruoli di responsabilità, è coinvolto, in qualsiasi forma, in attività commerciali e/o consulenziali verso l'Ente committente, è tenuto a redigere ed aggiornare mensilmente un report nel quale registra, in forma sintetica, tutti i contatti avuti con Responsabili dell'Ente, anche di tipo informale, riportando (oltre alle ovvie circostanze di data, orario, luogo e persone presenti), i contenuti e gli eventuali esiti di tali contatti. Tali evidenze andranno opportunamente conservate, da parte di ciascun Redattore, per essere rese disponibili a richiesta della Direzione Processi e Audit Interno o dell'Organismo di Vigilanza.
- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta: - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01; - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.
- Nel caso di fornitura resa all'Ente committente da un RTI/ATI a cui partecipa una Società del Gruppo Engineering, è severamente vietato attuare tra i Partner compensazioni economiche in forma tacita. Eventuali compensazioni economiche, in qualsiasi forma esse si attuino, dovranno avere forma esplicita, motivata e debitamente formalizzata.
- Gli atti formali di costituzione di un RTI/ATI (Costituzione RTI/ATI, Mandato speciale di rappresentanza, Accordo/Regolamento interno) possono essere sottoscritti SOLO da chi è intestatario di formale procura che definisce, fra l'altro, eventuali limiti economici relativi all'importo "firmabile".
- In tutti i casi in cui l'assunzione di personale determini l'erogazione pubblica di finanziamenti e/o decontribuzioni, la Direzione del Personale è tenuta, prima dell'assunzione, a verificare l'esistenza di tutti i requisiti oggettivi e soggettivi necessari per la fruizione delle agevolazioni. Le schede di valutazione devono contenere, per ogni Candidato, la sintesi del processo di valutazione e devono essere sottoscritte da almeno due Valutatori, appartenenti a strutture diverse dell'organizzazione. Tutta la documentazione relativa alla presenza dei requisiti oggettivi e soggettivi del personale per il quale l'azienda usufruisca di agevolazioni finanziare, deve essere verificata dalla Direzione del Personale e dalla stessa conservata in appositi archivi.

2.3.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
01 – 01	Alla stesura della Risposta al bando di gara (o dell'Offerta) partecipano, con ruoli diversi, diversi Responsabili, tecnici e commerciali. Sono previste obbligatoriamente fasi di approvazione formale dei contenuti tecnici, dei preventivi dei costi e dei ricavi, approvazioni demandate a Responsabili appartenenti a strutture diverse dell'organizzazione aziendale. La versione finale della Risposta al bando di gara (o Offerta), compresi i relativi allegati, devono essere verificati, in termini formali e sostanziali, dal Responsabile Commerciale coinvolto (o, se applicabile, dal Responsabile della Direzione Ricerca & Sviluppo) prima della trasmissione all'Ente pubblico. In particolare viene verificato che la Risposta al bando soddisfi i requisiti, soggettivi ed oggettivi, richiesti nel bando, che non contenga omissioni, imprecisioni o informazioni non vere.	**- PGA10 Gestione Contributi per la Ricerca** **- PGA03 Gestione Ciclo Attivo** **- PGA04 Gestione Preventivo Fornitura** **- RS03P02 Procedura Avvio Chiusura Attività** **- RS01P01 Procedura Gestione Acquisizione Contratti**
01 – 02	Le sottoscrizioni, da parte di un Rappresentante della Società: - di un'Offerta, di una *Risposta ad un bando di gara* o di un Contratto, verso un Cliente (ciclo attivo), ovvero - di un Contratto o di un Ordine, verso un Fornitore (ciclo passivo) sono atti formali che impegnano l'Azienda verso l'esterno; in quanto tali, non possono essere effettuati se non da chi è intestatario di apposita procura scritta, che definisce, fra l'altro, eventuali limiti economici relativi all'importo "firmabile". La titolarità di procure non esime il detentore delle stesse dal rispetto degli adempimenti aziendali prescritti per quanto concerne il processo autorizzativo interno.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo**
01 – 03	Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore la procedura "Gestione Procure/Deleghe" che fissa le norme per il conferimento e l'impiego di procure e deleghe utilizzate nel processo di formalizzazione contrattuale. In particolare, le deleghe possono essere rilasciate dai Procuratori Commerciali entro i limiti della propria procura e sotto la propria responsabilità, solo ed esclusivamente nell'ambito del Ciclo Attivo e per operare con soggetti privati.	**- PGA14 Gestione Procure Deleghe**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
01 – 04	Nell'ambito: → di una fornitura a beneficio di un Ente Pubblico, oppure → di una fornitura che preveda finanziamenti, sovvenzioni o contributi erogati da un Ente pubblico: - la stima dei costi preventivati (che devono risultare riconciliabili con la Risposta al bando, anche in termini di profili professionali impiegati nella fornitura), - la rendicontazione dei costi sostenuti, - la rendicontazione dello Stato Avanzamento Lavori devono scaturire da processi documentati, durante i quali vengono applicati criteri definiti ed oggettivi, in coerenza con i requisiti della fornitura. Il Responsabile Tecnico della fornitura è tenuto a verificare e, se necessario, a fare debitamente autorizzare dai propri Responsabili i risultati scaturiti dai processi. La documentazione che descrive i processi di stima e di rendicontazione, il dettaglio delle informazioni di input utilizzate ed il risultato prodotto vanno archiviati in luogo ad accesso limitato per almeno un anno dal mese di chiusura della commessa. Nell'ambito di una fornitura che veda come beneficiario finale una Pubblica Amministrazione o un Concessionario di pubblici finanziamenti, va garantita la tracciabilità dei flussi finanziari, nel rispetto di quanto previsto dalla L. 136/10.	**- PGA10 Gestione Contributi per la Ricerca** **- PGA02 Gestione Ciclo Passivo** **- RS03P02 Procedura Avvio Chiusura Attività** **- RS03P03 Procedura Esecuzione Controllo Attività**
01 – 05	Nell'ambito di una fornitura che preveda l'erogazione di corsi di formazione con beneficio di finanziamenti, sovvenzioni o contributi erogati da un Ente pubblico, il processo di valutazione e selezione dei potenziali Discenti deve essere condotto da almeno due Commissari, sulla base dei requisiti prescritti dall'Ente finanziatore ed applicando criteri definiti ed oggettivi, producendo, all'esito del processo, adeguata documentazione dello stesso, che va archiviata in luogo ad accesso limitato per almeno un anno dal mese di chiusura della commessa.	**- PGA10 Gestione Contributi per la Ricerca**
01 – 06	Nell'ambito di una fornitura che preveda finanziamenti, sovvenzioni o contributi erogati da un Ente pubblico, tutte le circostanze utili a descrivere nel dettaglio la natura e le modalità di svolgimento delle attività sono oggetto di adeguata registrazione. Ad esempio, nel caso di fornitura di un corso di formazione che preveda finanziamenti: → nome, profilo/titolo di studio, giorni di presenza e valutazione finale dei Docenti; → nome, profilo/titolo di studio, giorni di presenza e valutazione finale dei Discenti; → giorni/orario delle lezioni tenute, argomenti svolti, ecc. Sempre con riferimento al caso di fornitura di un corso di formazione, deve essere registrata anche l'avvenuta consegna, ai Discenti, del programma formativo conforme ai requisiti approvati dall'Ente finanziatore. Tali registrazioni vanno archiviate in luogo ad accesso limitato per almeno un anno dal mese di chiusura della commessa	**- PGA10 Gestione Contributi per la Ricerca** **- RS02P02 Procedura Gestione Fornitori**
01 – 07	Internamente all'Azienda va formalmente assegnato, a un Dipendente, il ruolo di Responsabile della commessa/Capo Progetto.	**- RS03P02 Procedura Avvio Chiusura Attività**
01 – 08	Nell'ambito dell'erogazione di una fornitura allo Stato, ad altro Ente Pubblico o Comunitario, vanno adottati, laddove il contesto li renda applicabili, i protocolli previsti per i reati-presupposto di cui all'art. 24-bis (commi 1, 2 e 3) del D.Lgs 231/01 (Delitti informatici e trattamento illecito di dati).	**- RS03P03 Procedura Esecuzione Controllo Attività** **- PGP03 Gestione Accesso ai Sistemi Aziendali** **- RGP01 Regolamento uso risorse rete**

2.4 Delitti informatici e trattamento illecito di dati (Art. 24-bis del D.Lgs. 231/01)

2.4.1 Reati richiamati dal D.Lgs. 231/01

Il primo comma dell'art. 24-bis del Decreto richiama specificatamente i seguenti reati.

- Accesso abusivo ad un sistema informatico o telematico
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- Danneggiamento di informazioni, dati e programmi informatici
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- Danneggiamento di sistemi informatici o telematici
- Danneggiamento di sistemi informatici o telematici di pubblica utilità

Il secondo comma dell'art. 24-bis del Decreto richiama specificatamente i seguenti reati:

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Il terzo comma dell'art. 24-bis del Decreto richiama specificatamente i seguenti reati.

- Falsità in un documento informatico pubblico o avente efficacia probatoria
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti:

- con riferimento alle fattispecie di cui al **primo comma** dell'art. 24 bis del D. Lgs. 231/2001:
  - Introduzione in un sistema informatico, interno e/o esterno all'Azienda, violandone il sistema di sicurezza, ovvero operare al suo interno contro la volontà, espressa o tacita, di chi ha il diritto di escluderlo
  - Intercettazione, impedimento o interruzione fraudolenta di comunicazioni informatiche/telematiche (interne od esterne all'Azienda); diffusione pubblica, anche solo parziale, mediante qualsiasi mezzo di informazione, del contenuto delle comunicazioni
  - Installazione, fuori dai casi previsti (da leggi, procedure o contratti) di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche/telematiche (interne od esterne all'Azienda)
  - Distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui; ovvero commissione di tali atti su informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
- Con riferimento al **secondo comma** dell'articolo in commento:
  - Reperimento, riproduzione, diffusione, comunicazione o consegna abusiva di codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, interno od esterno all'Azienda, protetto da misure di sicurezza; dare indicazioni o istruzioni idonee al predetto scopo, al fine di procurare a sé o ad altri un profitto o arrecare ad altri un danno
  - Reperimento, produzione, riproduzione, importazione, diffusione, comunicazione, consegna o, comunque, messa a disposizione di altri di apparecchiature, dispositivi o programmi informatici

(anche prodotti da altri), con lo scopo di danneggiare un sistema informatico o telematico (interno od esterno all'Azienda), le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per provocare l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

- Con riferimento al **terzo comma** dell'articolo in commento:
  - in relazione ad un documento informatico pubblico o privato: falsificazione di documenti informatici o, comunque, uso di documenti informatici falsi.
  - nell'ambito della fornitura di un servizio di certificazione di firma elettronica: violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato, con lo scopo di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

Nota: per *documento informatico* si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

2.4.2 Contestualizzazione aziendale e modalità di commissione

L'art. 24-bis del D.Lgs. 231/01 elenca, nei 3 commi che lo compongono, 11 distinti reati previsti dal Codice Penale, tutti attinenti al settore informatico.

Data la natura del suo *core business*, appare evidente la particolare esposizione che la Società presenta rispetto all'ipotesi di compimento dei reati qui trattati.

Ciò, in particolare, tenendo conto delle seguenti due circostanze, astrattamente in grado di "agevolare" la commissione di atti illeciti:

- le competenze tecniche indispensabili per il compimento dei reati qui considerati sono possedute da molte delle persone che lavorano per l'Azienda;
- nell'ambito delle attività inerenti una fornitura, spesso il personale Dell'Azienda opera "all'interno" dell'infrastruttura informatica del proprio Cliente, avendo frequentemente la possibilità/necessità (regolamentata dal contratto) di accedere ad apparecchiature e dati del Cliente stesso.

Le gravi sanzioni che la legge infliggerebbe alla Società nell'ipotetica eventualità di commissione di uno dei reati informatici qui considerati, sarebbero sempre di due tipi:

- sanzioni pecuniarie
- sanzioni interdittive; queste potranno andare, ad esempio, dal divieto di pubblicizzare beni o servizi, al divieto di contrattare con la Pubblica Amministrazione, fino all'interdizione dall'esercizio dell'attività.

Va tenuto presente che eventuali sanzioni di legge che fossero comminate all'Azienda esporrebbero la stessa ad un ulteriore danno, di assoluto rilievo: il *danno reputazionale*. Tale danno potrebbe venir a gravare sull'immagine dell'intero Gruppo Engineering.

È opportuno aggiungere che la legge prevede l'applicazione, nei confronti dell'Ente, di aggravanti, anche in termini sanzionatori, nelle seguenti due specifiche circostanze:

- se l'infrazione è posta in essere da personale che agisce nel ruolo di operatore/gestore del sistema
- se le informazioni, i dati o i sistemi informatici oggetto di interventi illeciti sono utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità.

Alla luce delle precedenti considerazioni, La Società ha ritenuto di considerare i reati informatici "*reati di particolare rilevanza*" e di sanzionarli con maggior severità nell'ambito del *sistema disciplinare* descritto nel presente Modello.

Va sottolineato che, ancorché il presupposto dell'*interesse e vantaggio* ottenuto dall'Azienda a seguito della commissione del reato (presupposto che caratterizza l'imputabilità di un Ente ex D.Lgs. 231/01)

porti (implicitamente) ad identificare, come parte offesa, il Cliente dell'Azienda (in particolare: il suo Sistema Informatico, le infrastrutture, le informazioni ed i dati gestiti), il presente *Modello*, come ulteriore misura volta a minimizzare il rischio di compimento del reato, applica le norme, i protocolli ed i controlli di seguito riportati anche con riferimento al proprio Sistema Informatico, alle infrastrutture, alle informazioni ed ai dati gestiti da tale Sistema.

Da tutto quanto precede scaturisce la considerazione che, rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è talmente pervasivo che non ha particolare significato indicare specifici **Soggetti/UU.OO**. **sensibili**, fatto salvo quanto di seguito indicato con riferimento alle fattispecie di reato richiamate dal terzo comma (si veda in seguito).

Analogamente per quanto riguarda i **processi/sottoprocessi sensibili**: il rischio di compimento del reato-presupposto qui considerato è pervasivo e quindi non risulta associabile a specifici processi, anche qui fatto salvo quanto di seguito specificato trattando il terzo comma.

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare con riferimento alle fattispecie di cui al **primo comma** dell'articolo in commento, sono le seguenti.

- Ci si introduce nel Sistema Informatico ("S.I.") dell'Azienda, di un Cliente o di un Fornitore, sistema protetto da misure di sicurezza, con modalità e per finalità non autorizzate da chi ha inteso proteggere il sistema.
- Si interviene illecitamente, eventualmente mediante l'installazione di apposite apparecchiature, sul flusso di comunicazione fra sistemi dell'Azienda, di Clienti o di Terze Parti, intercettando, impedendo o interrompendo tale flusso. Eventualmente l'intervento di cui sopra viene seguito dalla diffusione, anche parziale, del contenuto delle comunicazioni.
- Allo scopo di rendere in tutto o in parte inservibili i S.I. altrui, si interviene illecitamente modificando o cancellando dati, informazioni o programmi informatici ovvero si introducono/trasmettono dati, informazioni o programmi:
  - ✓ presenti nei sistemi di Clienti o Terze Parti,
  - ✓ utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

alle fattispecie di cui al **secondo comma** dell'articolo in commento, si ritiene opportuno richiamare quanto illustrato in sede di trattazione del reato di cui all'art. 24-bis – comma 1, a cui si rimanda.

È importante evidenziare che, per quanto riguarda lo svolgimento di processi autorizzativi interni alla Società, la cessione ad altri dei propri codici personali di accesso al S.I.I. (*credenziali*) ovvero l'acquisizione fraudolenta di *credenziali* altrui, possono costituire atti strumentali per il perfezionamento di altro diverso reato previsto dal D.Lgs. 231/01. Si pensi, ad esempio, all'autorizzazione di un illecito pagamento finalizzato ad un tentativo di corruzione.

Con riferimento alle fattispecie di cui al terzo comma dell'articolo in commento, premesso che relativamente al reato di "*Frode informatica del certificatore di firma elettronica*", attualmente tale reato non risulta neppure astrattamente ipotizzabile in Azienda, non essendo prevista la tipologia di fornitura richiamata, rispetto al reato di "*Falsità in documento informatico pubblico o avente efficacia probatoria"* l'esposizione al rischio della Società si osserva soprattutto con riferimento ai seguenti **Soggetti/UU.OO**. **sensibili**:

- Dir. Gen. P.A. e Sanità,
- Scuola di IT & Management "ENRICO DELLA VALLE"
- Dir. Gen. Human Resource & Organization
- Dir. Gen. Ricerca e Innovazione
- Dir. Gen. Amm. Fin. e Controllo

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Erogazione di una fornitura nei confronti dello Stato, di un Ente Pubblico o Comunitario/Intervento sulle informazioni che concorrono alla formazione di un documento informatico prodotto sotto la responsabilità del Cliente
- Rapporti con l'Amministrazione dello Stato, di un Ente Pubblico o Comunitario/Trasmissione di informazioni registrate in un documento informatico.

Le modalità di commissione del reato che si possono astrattamente ipotizzare sono le seguenti.

- Un Dipendente o un Consulente impegnato nell'erogazione di una fornitura a favore dello Stato o di un Ente Pubblico o Comunitario, sfruttando la detenzione di abilitazioni giustificate dalle attività previste dalla tipologia di fornitura, interviene sulle informazioni contenute/elaborate dal Sistema Informatico del Cliente, con lo scopo di far sì che venga prodotto un documento informatico dal contenuto totalmente o parzialmente falso.
- Nei rapporti intrattenuti dalla Società con una Pubblica Amministrazione, si predispongono documenti informatici falsi.

2.4.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.4.3.1 Principi specifici di comportamento

- I soggetti sopra indicati sono tenuti a rispettare scrupolosamente tutte le norme vigenti, ed in particolare:
  - utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
  - custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
  - garantire la tracciabilità delle operazioni di inserimento/modifica effettuate in relazione al sistema delle abilitazioni/deleghe interne utilizzato in Azienda;
  - assicurare meccanismi di protezione dei file, quali, ad esempio, password da aggiornare periodicamente, secondo le prescrizioni comportamentali della Società;
  - utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;
  - utilizzare unicamente materiale pubblicitario (i.e. materiale fotografico) autorizzato.

- In aggiunta a quanto sopra previsto, ai Destinatari del Modello è fatto divieto di:
  - utilizzare le risorse informatiche (es. personal computer fissi o portatili) assegnate dalla Società in violazione delle norme aziendali in vigore;
  - effettuare download illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;
  - alterare documenti elettronici, pubblici o privati, con finalità probatoria;
  - accedere, senza averne l'autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);

- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi: codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui, protetto da misure di sicurezza;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- aggirare o tentare di aggirare i sistemi di sicurezza aziendali (es: Antivirus, Firewall, Proxy server, etc.);
- lasciare il proprio Personal Computer incustodito e senza protezione *password;*

➢ In qualunque contesto, ma in particolar modo nell'ambito dell'erogazione di una fornitura allo Stato, ad altro Ente Pubblico o Comunitario, anche avendo la possibilità di accedere lecitamente al Sistema Informatico ("S.I.") del Cliente, ovvero all'infrastruttura tecnologica, alle applicazioni, ai programmi, ai dati ed alle informazioni pertinenti a tale S.I., è assolutamente vietato intervenire, in qualunque modo, allo scopo ultimo di falsificare un documento informatico pubblico o avente efficacia probatoria. E' altresì vietato utilizzare documenti informatici falsi.

2.4.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
02 – 01	Un Sistema Informatico ("*S.I.*"), con ciò intendendo la sua infrastruttura tecnologica, le sue applicazioni, i suoi programmi, i dati e le informazioni ad esso pertinenti, indipendentemente dal fatto che si tratti del S.I. della Società, di un Cliente o di una Terza Parte, può essere *acceduto* effettuando *intercettazioni*, *consultazioni, duplicazioni* o *modifiche* (intervenendo, in qualunque modo, su di esso) ***solo ed esclusivamente*** previa legittima acquisizione delle previste autorizzazioni ed esclusivamente con modalità e per finalità che risultino coerenti con il ruolo svolto e, in ambito contrattuale, con quanto previsto dal contratto.	**- PGT01 Gestione Privacy** **- MSGTD Manuale Gestione Trattamento Dati Personali** **- RS03P03 Procedura Esecuzione Controllo Attività** **- RGP01 Regolamento uso risorse rete**
02 – 02	Chiunque operi in nome o per conto della Società è direttamente responsabile, civilmente e penalmente, a norma delle leggi vigenti, per l'uso fatto della rete aziendale, del servizio internet e della posta elettronica. Tale responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.	**- RGP01 Regolamento uso risorse rete**
02 – 03	L'applicazione informatica che controlla l'accesso ai Sistemi aziendali deve essere gestita centralmente rispettando rigorosi criteri di: ==> definizione delle responsabilità ==> separazione delle funzioni ==> limitazione dell'accesso ai soli dati che risultano essenziali e strettamente necessari ciò allo scopo di garantire la sicurezza/protezione dei sistemi, la riservatezza e l'integrità dei dati in coerenza con le mansioni affidate a coloro che ne hanno accesso. L'applicazione che controlla l'accesso ai Sistemi aziendali deve tener traccia di tutti i tentativi di accesso al sistema.	**- PGP03 Gestione Accesso ai Sistemi Aziendali**
02 – 04	Il Responsabile (titolare di CdC) di una Risorsa che ha necessità di accedere al S.I. interno, deve chiedere, tramite l'apposita applicazione informatica, il censimento del nuovo Utente, specificando il profilo di abilitazioni che deve essere a lui assegnato. La Direzione del Personale deve comunicare regolarmente al Responsabile della gestione del sistema di accesso i nomi di Dipendenti/Collaboratori che hanno cessato la loro attività in Azienda, chiedendo con ciò la disattivazione delle rispettive utenze.	**- PGP09 Gestione Risorse Umane** **- PGP03 Gestione Accesso ai Sistemi Aziendali**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
02-05	L'applicazione informatica che controlla l'accesso ai Sistemi aziendali deve essere gestita centralmente rispettando rigorosi criteri di protezione e sicurezza definiti in apposita Procedura. Sia operando in Azienda che presso un Cliente o un Fornitore, i codici di accesso (user-ID e password) assegnati all'Utente vanno trattati come *strettamente personali* e non vanno messi a conoscenza di alcuno. E' vietato agire allo scopo di venire illecitamente a conoscenza dei codici personali di accesso di un altro Utente e/o allo scopo di diffondere gli stessi. Se si venisse a conoscenza, per cause fortuite, di codici personali altrui, oltre al divieto assoluto di utilizzarli, v'è l'obbligo di informare immediatamente di tale circostanza l'Utente titolare dei codici stessi, che provvederà all'immediata modifica (almeno) della propria password.	**- PGA02 Gestione Ciclo Passivo** **- PGP09 Gestione Risorse Umane** **- PGP03 Gestione Accesso ai Sistemi Aziendali** **- RGP01 Regolamento uso risorse rete**
02-06	Nell'ambito del S.I. aziendale e facendo uso dell'infrastruttura tecnologica (server, PC, ecc.), della rete, dei sevizi (compresa e-mail) e/o delle applicazioni aziendali, è vietato: → acquisire o diffondere materiale illegale o con contenuti offensivi → ricevere, installare, diffondere, usare software protetto da copyright (a meno che non sia espressamente consentito dalla licenza d'uso) o software finalizzato ad eludere o forzare i sistemi di protezione rispetto ai tentativi di copia/duplicazione → qualsiasi operazione finalizzata a compromettere l'integrità dei dati, la privacy, la riservatezza, la sicurezza, la funzionalità o le prestazioni di sistemi informatici (anche di singole apparecchiature), eventualmente eludendo o forzando i sistemi di controllo → qualsiasi altra attività vietata dalla legislazione vigente	**- RGP01 Regolamento uso risorse rete**
02-07	Il traffico di rete va filtrato e tracciato su file di log, i quali vengono conservati a termini di legge per consentire all'Autorità Giudiziaria di effettuare indagini su eventuali reati, nel rispetto della normativa vigente a tutela dei diritti dei Lavoratori. Il personale tecnico, che deve essere debitamente ed opportunamente autorizzato dall'Azienda, avrà accesso ai dati di traffico al fine di garantire il corretto ed ottimale funzionamento della rete e dei servizi	**- RGP01 Regolamento uso risorse rete**

2.5 Delitti di criminalità organizzata (Art. 24-ter del D.Lgs. 231/01)

2.5.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 24-ter del Decreto richiama specificatamente i seguenti articoli del Codice Penale.

- Associazione per delinquere
- Associazioni di tipo mafioso anche straniere
- Scambio elettorale politico-mafioso
- Sequestro di persona a scopo di rapina o di estorsione
- Associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope
- Delitti concernenti l'illegale fabbricazione, introduzione nello Stato, 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

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

- Ci si associa allo scopo di commettere più reati
- Si fa parte di un'associazione di tipo mafioso
- Si ottiene la promessa di voti in cambio della erogazione di denaro
- Si sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto
- Si fa parte di un'associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

(Per l'ultimo dei reati precedentemente elencati - detenzione/traffico illegale di armi - si rimanda alla descrizione già fornita).

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere reati, per acquisire la gestione o il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri. Le disposizioni del presente articolo si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

2.5.2 Contestualizzazione aziendale e modalità di commissione

Da un'analisi delle attività nel cui ambito possono essere commessi i reati elencati, è emersa l'inapplicabilità alla Società delle fattispecie delittuose di cui agli artt. 416 comma 6, 416-ter, 630 c.p., 74 D.P.R. n. 309/1990, 407 comma 2 lett. a) n. 5 c.p.p. Si tratta, infatti, di fattispecie penali da considerare del tutto estranee alle attività di impresa svolta dalla Società, nonché assolutamente contrarie ai valori e principi che ne hanno da sempre ispirato l'agire, rispetto alle quali non è, pertanto, necessario predisporre alcuna misura preventiva o richiamare specifici principi generali di comportamento.

Un discorso in parte differente va fatto per quel che riguarda l'associazione per delinquere di cui all'art. 416 c.p., i cui elementi costitutivi tipici si fondano sulla stabilità del vincolo associativo, desumibile da un certo livello di organizzazione dell'associazione e dal perseguimento di una finalità associativa consistente nella realizzazione di un programma delittuoso generico, di commettere cioè una serie indeterminata di delitti.

Sullo specifico punto, è intervenuta la Suprema Corte circoscrivendo l'operatività dell'art. 24 ter, negando la possibilità di recuperare indirettamente i delitti-scopo del reato associativo; a ragionare diversamente, infatti, "*la norma incriminatrice di cui all'art. 416 c.p. si trasformerebbe, in violazione del principio di tassatività del sistema sanzionatorio contemplato dal D.Lgs. n. 231 del 2001, in una disposizione "aperta", dal contenuto elastico, potenzialmente idoneo a ricomprendere nel novero dei reati-presupposto qualsiasi fattispecie di reato, con il pericolo di un'ingiustificata dilatazione dell'area di potenziale responsabilità dell'ente collettivo, i cui organi direttivi, peraltro, verrebbero in tal modo costretti ad adottare su basi di assoluta incertezza e nella totale assenza di oggettivi criteri di riferimento, i modelli di organizzazione e di gestione previsti dal citato D.Lgs., art. 6, scomparendone, di fatto, ogni efficacia in relazione agli auspicati fini di prevenzione*" (Cassazione penale, Sez. VI, 20 dicembre 2013, n. 3635).

Ebbene, esclusa la possibilità di immaginare nel caso della Società e, più in generale, di ogni impresa lecita, la realizzazione della condotta di costituzione di una associazione a ciò finalizzata, si tratta di vagliare il rischio che la struttura organizzativa societaria sia utilizzata da più persone al fine di realizzare una serie di delitti nell'interesse o a vantaggio della Società stessa; ipotesi che la giurisprudenza spesso riconduce alla figura dell'art. 416 c.p., piuttosto che al mero concorso di persone in più reati.

In quest'ottica, è evidente come il rischio che ciò accada non sia individuabile ex ante da parte della Società, ma si leghi ad un fenomeno di devianza dipendente dalla determinazioni di alcuni suoi membri, nel caso in cui decidano di sfruttare l'organizzazione di persone e di mezzi, tipica di ogni impresa, per fini criminali.

Le misure preventive immaginabili sono legate, in primo luogo, alla diffusione più ampia possibile della filosofia di impresa perseguita dalla Società, ribadendo a chiunque operi al suo interno che il perseguimento di vantaggi per la Società, ottenuti attraverso il compimento di attività penalmente vietate,

non è mai consentito e che la Società adotterà ogni misura, anche radicale, ritenuta utile a garantire immediatamente in quel settore organizzativo la situazione di legalità e trasparenza, nell'ipotesi in cui emerga il fondato sospetto che soggetti operanti nella società siano dediti alla commissione di fatti delittuosi, seppure a vantaggio della Società stessa.

Tuttavia, al solo fine di scongiurare il pur remoto rischio che per la devianza di singoli soggetti operanti all'interno della società, si possano in qualche modo agevolare dall'esterno, mediante il perfezionamento di rapporti contrattuali, organizzazioni di tipo criminale, si è ritenuto utile richiamare i principi di base e le regole della libera concorrenza - che hanno, peraltro, ispirato da sempre la filosofia di impresa della Società – per esigerne il rispetto.

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che le aree a rischio di seguito menzionate devono intendersi integrate con le altre specificatamente individuate in relazione a ciascuna fattispecie oggetto di trattazione nelle altre Parti Speciali del presente Modello.

Tale precisazione si ritiene necessaria per ragioni strettamente legate alla formazione di un Modello quanto più efficace e in linea con il dettato normativo del D.Lgs. 231/01.

Ciò precisato, rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Vertice aziendale
- Dir. Gen. Amm. Fin. e Controllo
- Direzioni commerciali
- Direzioni tecniche di produzione

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Ciclo Passivo (acquisti ed approvvigionamenti)
- Ciclo Attivo (vendite)

In particolare, relativamente al Ciclo Attivo:

- Partecipazione ad una gara: attività preliminari alla formalizzazione della Risposta al bando; formalizzazione della Risposta
- Gestione Amministrativa RTI-ATI/Gestione rapporti economici fra Partner.

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- In via del tutto generale: allacciamento e mantenimento di rapporti d'affari, economici o commerciali, di natura delittuosa con l'organizzazione di un Cliente, di un Fornitore o di un Partner.
- Attuazione di irregolari compensazioni economiche fra Partner di un RTI/ATI, finalizzate alla commissione dei reati qui considerati.
- Produzione e/o vendita di sistemi d'arma (o parti di sistemi d'arma; ad esempio: sistemi software utilizzati in apparati lanciamissili), nei casi in cui il rapporto con il Committente specifico o le procedure di cessione/vendita adottate siano vietati da leggi, convenzioni o determinazioni vigenti ed applicabili.

2.5.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.5.3.1 Principi specifici di comportamento

- Durante la fase che precede l'emissione di un bando di gara ed in quella di partecipazione alla stessa, il personale di una Società del Gruppo Engineering che, con ruoli di responsabilità, è coinvolto, in qualsiasi forma, in attività commerciali e/o consulenziali verso l'Ente committente, è tenuto a redigere ed aggiornare mensilmente un report nel quale registra, in forma sintetica, tutti i contatti avuti con Responsabili dell'Ente, anche di tipo informale, riportando (oltre alle ovvie circostanze di data, orario, luogo e persone presenti), i contenuti e gli eventuali esiti di tali contatti. Tali evidenze andranno opportunamente conservate, da parte di ciascun Redattore, per essere rese disponibili a richiesta della Direzione Processi e Audit Interno o dell'Organismo di Vigilanza;
- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
  - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.
- Nel caso di fornitura resa all'Ente committente da un RTI/ATI a cui partecipa una Società del Gruppo Engineering, è severamente vietato attuare tra i Partner compensazioni economiche in forma tacita. Eventuali compensazioni economiche, in qualsiasi forma esse si attuino, dovranno avere forma esplicita, motivata e debitamente formalizzata.

2.5.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
03 – 01	Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai processi sensibili rientranti nelle procedure di seguito elencate: → Gestione Anagrafica Fornitori: qualificazione e censimento nuovi Fornitori/modifica dati anagrafici e riferimenti bancari → Gestione Albo Fornitori qualificati: selezione Fornitori da Albo, valutazione Fornitori qualificati ed aggiornamento Albo → Gestione Ciclo passivo: autorizzazione alla spesa, stesura, analisi e sottoscrizione contratto, gestione fatturazione passiva e mandati di pagamento → Gestione Ciclo attivo: verifica e autorizzazione preventivi costi-ricavi, analisi e sottoscrizione contratto, gestione fatturazione attiva → Gestione Anagrafica Clienti: censimento nuovi Clienti/modifica dati anagrafici Nell'ambito di una fornitura che veda come beneficiario finale una Pubblica Amministrazione o un Concessionario di pubblici finanziamenti, va garantita la tracciabilità dei flussi finanziari, nel rispetto di quanto previsto dalla L. 136/10. In linea generale, deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Va sottoposta a gestione centrale controllata la tabella contenente i nomi dei Responsabili intestatari di delega all'autorizzazione delle richiesta d'acquisto, tabella utilizzata dalla procedura informatica che gestisce il ciclo autorizzativo. Analoga gestione controllata e centralizzata va adottata per la tabella contenente i nomi dei Responsabili che possono autorizzare l'emissione di un'Offerta/Contratto di vendita. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- RS01P01 Procedura Gestione Acquisizione Contratti** **- RS02P01 Procedura Gestione Offerta Prima Qualificazione Fornitori** **- RS02P02 Procedura Gestione Fornitori**
03 – 02	Le sottoscrizioni, da parte di un Rappresentante della Società: - di un'Offerta, di una *Risposta ad un bando di gara* o di un Contratto, verso un Cliente (ciclo attivo), ovvero - di un Contratto o di un Ordine, verso un Fornitore (ciclo passivo) sono atti formali che impegnano l'Azienda verso l'esterno; in quanto tali, non possono essere effettuati se non da chi è intestatario di apposita procura scritta, che definisce, fra l'altro, eventuali limiti economici relativi all'importo "firmabile". La titolarità di procure non esime il detentore delle stesse dal rispetto degli adempimenti aziendali prescritti per quanto concerne il processo autorizzativo interno.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
03 – 03	Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore la procedura "Gestione Procure/Deleghe" che fissa le norme per il conferimento e l'impiego di procure e deleghe utilizzate nel processo di formalizzazione contrattuale. In particolare, le deleghe possono essere rilasciate dai Procuratori Commerciali entro i limiti della propria procura e sotto la propria responsabilità, solo ed esclusivamente nell'ambito Ciclo Attivo e per operare con soggetti privati. All'atto del conferimento di una delega devono, in ogni caso, essere rispettati i limiti di valore – dipendenti dal ruolo aziendale del soggetto delegato - così come definiti in apposita tabella pubblicata nella intranet aziendale. Nella stessa rete intranet è reperibile il modello che deve essere obbligatoriamente impiegato per la formalizzazione di una delega.	**- PGA14 Gestione Procure Deleghe**

2.6 Concussione, induzione indebita a dare o promettere utilità e corruzione (Art. 25 del D.Lgs. 231/01)

Prima di entrare nel merito della presente parte speciale, si ritiene opportuno dare atto di un approfondimento svolto di recente dalla Capogruppo.

In considerazione della partecipazione al Gruppo Engineering, anche di società con sede legale all'estero e operanti al di fuori del territorio nazionale, nonché alla luce della nuova compagine sociale soggetta alla giurisdizione statunitense, la Capogruppo ha ritenuto opportuno verificare la conformità del Modello adottato, rispetto alla normativa anticorruzione vigente negli Stati Uniti d'America (c.d. "*Foreign Corrupt Practices Act*" o anche "F.C.P.A.") e nel Regno Unito (c.d. "*Bribery Act*").

Partendo dall'analisi del D.Lgs. 231/01, con particolare riferimento alle fattispecie di corruzione pubblica e privata, esaminando i punti cardine della normativa anticorruzione contenuti nel "F.C.P.A.", con specifico riguardo ai c.d. "*Hallmarks of effective Compliance Programs*", nonché le procedure e regole di condotta previste dalla "*Bribery Act",* il Modello adottato dalla Società nella parte di interesse (reati contro la pubblica amministrazione e reati societari), unitamente al sistema di presidi e di controlli in essere, risultano assolutamente *compliant*, tanto alla normativa nazionale, quanto in relazione al F.C.P.A. e al Bribery Act.

Trattandosi delle medesime procedure aziendali, tale Risk Assessment può essere esteso, in termini di ulteriore presidio, anche ad Engineering D.HUB.

2.6.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25 del Decreto richiama specificatamente i seguenti articoli del Codice Penale.

- Concussione (art. 317)
- Corruzione per l'esercizio della funzione (art. 318)
- Corruzione per un atto contrario ai doveri di ufficio (art. 319)
- Corruzione per un atto contrario ai doveri d'ufficio aggravato ai sensi dell'art. 319-bis
- Corruzione in atti giudiziari (art. 319-ter)
- Induzione indebita a dare o promettere utilità (art. 319-quater)
- Corruzione di persona incaricata di un pubblico servizio (art. 320)
- Pene per il corruttore (art. 321)

- Istigazione alla corruzione (art. 322)
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis).

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

A) Si omette o si ritarda un atto d'ufficio, ovvero si compie un atto contrario ai doveri d'ufficio con il fine di ricevere, per sé o per un terzo, denaro od altra utilità o se ne accetta la promessa

B) Per le finalità appena menzionate, si sollecita una promessa o dazione di danaro o altra utilità

C) Viene commesso il reato di cui al punto (A) precedente finalizzato a favorire o danneggiare una parte in un processo civile, penale o amministrativo.

D) Abusando della qualità o dei poteri di pubblico ufficiale o di incaricato di pubblico servizio, si induce taluno a dare o a promettere indebitamente (a sé o a un terzo) denaro o altra utilità. Nella medesima circostanza, subendo la sollecitazione di un pubblico ufficiale o di un incaricato di pubblico servizio, si dà o si promette indebitamente denaro o altra utilità.

E) In relazione ai reati fin qui menzionati:

- si dà o si promette ad un pubblico ufficiale o ad un incaricato di pubblico servizio denaro o altra utilità

ovvero

- si induce un pubblico ufficiale o un incaricato di pubblico servizio alla commissione di uno dei reati sopra citati.

F) Le fattispecie di reati fin qui considerati vengono commesse da chi, o nei confronti di chi, nell'ambito di altri Stati esteri (comunitari o extra-europei), svolga funzioni o attività corrispondenti a quelle di pubblico ufficiale o di incaricato di un pubblico servizio.

Nota generale. Benché alcuni dei reati presupposto qui richiamati, siano *reati propri* di soggetti pubblici, non va tuttavia trascurata la circostanza che gli stessi reati potrebbero essere commessi da parte di Dipendenti Della Società in concorso con il soggetto qualificato o anche da chi, semplicemente, *svolge incarichi di pubblico servizio*, ruolo che potrebbe essere ipoteticamente ricoperto da Dipendenti che si trovassero ad erogare particolari forniture per un Cliente della P. A..

2.6.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Dir. Gen. P.A. e Sanità,
- Dir. Gen. Tecnica Innovazione e Ricerca

Infatti tali UU.OO. si rivolgono a settori di mercato perfettamente identificabili con i Soggetti richiamati da questo articolo del Decreto: Stato, Enti Pubblici e Istituzioni comunitarie.

Possono altresì risultare sensibili le seguenti UU.OO.:

- Scuola di IT & Management "ENRICO DELLA VALLE"
- Dir. Gen. Human Resource & Organization
- Dir. Gen. Amm. Fin. e Controllo.

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Ciclo Passivo (acquisti ed approvvigionamenti)/Stesura, autorizzazione e sottoscrizione contrattuale, Gestione fatturazione
- Gestione Acquisizione Consulenze Informatiche

- Ciclo Attivo/Partecipazione ad una gara: attività preliminari alla formalizzazione della Risposta al bando; formalizzazione della Risposta
- Ciclo Attivo/ Stesura, autorizzazione e sottoscrizione contrattuale
- Ciclo Attivo/ Gestione fatturazione
- Gestione Amministrativa RTI-ATI/Gestione rapporti economici fra Partner
- Gestione Cassa/Autorizzazione ai prelievi ed ai reintegri, Rendicontazione
- Gestione Servizi Finanziari e di Tesoreria/Gestione conti correnti bancari
- Gestione Risorse/Selezione ed assunzione di Personale
- Conferimento ed impiego di Procure-Deleghe di valenza esterna

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- Con riferimento al contesto che vede una Società del Gruppo entrare in contatto con un Funzionario/Rappresentante dell'amministrazione dello Stato o di un Ente Pubblico o Comunitario o a persone a queste collegabili, le seguenti attività potrebbero astrattamente configurarsi come di natura corruttiva, finalizzate, cioè, ad ottenere un indebito vantaggio o a ricompensare per il conseguimento dello stesso (quale può essere, ad es., l'aggiudicazione di una gara pubblica):

  a) acquisto di forniture o di prestazioni professionali (es.: apparati HW, consulenti, docenti, ecc.)

  b) assunzione di personale da parte di una Società del Gruppo o di altra Società compiacente

  c) offerta, donazione di beni, ad es.: orologi di valore, ecc.

  d) irregolari compensazioni economiche fra Partner di un RTI/ATI.

- Un'altra situazione teoricamente ipotizzabile è la seguente: un Dipendente del Gruppo Engineering impegnato nell'erogazione di una fornitura a favore di un Ente Pubblico, abusando della qualità o dei poteri a lui conferiti dal Cliente, che astrattamente gli consentono di inserire, modificare, cancellare od omettere dati e/o informazioni che concorrono alla formazione di atti o documenti emanati dalla P.A., richiede per sé o per terzi ovvero induce taluno ad offrire, a lui o a terzi, denaro o altra utilità a fronte di un suo intervento illecito sul Sistema Informativo del Cliente.
- In situazione analoga a quella sopra richiamata, un Dipendente del Gruppo Engineering:

  - sfruttando la qualità o i poteri a lui conferiti dal Cliente, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, ovvero
  - subendo la sollecitazione di un Pubblico Ufficiale o di un Incaricato di pubblico servizio, dà o promette indebitamente, denaro o altra utilità.

Si segnala infine che l' Azienda ha deciso di connotare come reati "*di particolare rilevanza*" gli eventuali reati commessi nell'ambito dei rapporti (preliminari o successivi alla formalizzazione contrattuale) instaurati con una Pubblica Amministrazione, *Centrale* o *Locale*, o con Istituzioni Comunitarie e di sanzionarli con maggior severità nell'ambito del *sistema disciplinare* descritto nel presente Modello.

2.6.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.6.3.1 Principi specifici di comportamento

- Le casistiche di comportamento (A, B e C) che di seguito vengono vietate, restano tali, ovvero "***vietate***" in quanto i comportamenti ipotizzati siano adottati nell'interesse o a vantaggio della Società.

  - A) A chiunque si presenti in nome o per conto di una Società del Gruppo Engineering è severamente vietato porre in essere atti finalizzati a corrompere un Funzionario/Rappresentante di un'Amministrazione dello Stato o di un Ente Pubblico o Comunitario, o un Incaricato di pubblico servizio.

- B) Ad un Soggetto che, per conto di una Società del Gruppo Engineering, si trovasse impegnato nella partecipazione ad una gara pubblica o nell'erogazione di una fornitura a favore di un Ente Pubblico, è severamente vietato richiedere per sé o per terzi ovvero indurre taluno ad offrire, a lui o a terzi, denaro o altra utilità, a fronte della commissione di un atto illecito.
- C) Ad un Soggetto che, per conto di una Società del Gruppo Engineering, si trovasse impegnato nell'erogazione di un servizio a favore di un Ente Pubblico, è severamente vietato:
  - ✓ abusando della qualità o dei poteri di Pubblico Ufficiale o di *Incaricato di pubblico servizio* (a lui eventualmente conferiti dal Cliente per l'erogazione del servizio), indurre taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità;
  - ✓ subendo la sollecitazione di un Pubblico Ufficiale o di un *Incaricato di pubblico servizio*, dare o promettere indebitamente denaro o altra utilità;

➢ Durante la fase che precede l'emissione di un bando di gara ed in quella di partecipazione alla stessa, il personale di una Società del Gruppo Engineering che, con ruoli di responsabilità, è coinvolto, in qualsiasi forma, in attività commerciali e/o consulenziali verso l'Ente committente, è tenuto a redigere ed aggiornare mensilmente un report nel quale registra, in forma sintetica, tutti i contatti avuti con Responsabili dell'Ente, anche di tipo informale, riportando (oltre alle ovvie circostanze di data, orario, luogo e persone presenti), i contenuti e gli eventuali esiti di tali contatti. Tali evidenze andranno opportunamente conservate, da parte di ciascun Redattore, per essere rese disponibili a richiesta della Direzione Processi e Audit Interno o dell'Organismo di Vigilanza.

➢ Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:

- che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
- l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.

➢ Nel caso di fornitura resa all'Ente committente da un RTI/ATI a cui partecipa una Società del Gruppo Engineering, è severamente vietato attuare tra i Partner compensazioni economiche in forma tacita. Eventuali compensazioni economiche, in qualsiasi forma esse si attuino, dovranno avere forma esplicita, motivata e debitamente formalizzata.

➢ Allo scopo di avere totale garanzia che nell'ambito del processo di selezione e assunzione del Personale, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), nel contesto del processo di valutazione del Candidato, vanno obbligatoriamente sottoscritte due distinte dichiarazioni, una del Candidato stesso, l'altra del Responsabile aziendale che lo ha sottoposto a colloquio di valutazione, dichiarazioni con le quali tali Soggetti, ciascuno sulla base delle informazioni a sua disposizione, attestano che il processo s'è svolto in assenza di illecite interferenze da parte di Terzi o per illecite finalità.

➢ Gli atti formali di costituzione di un RTI/ATI (Costituzione RTI/ATI, Mandato speciale di rappresentanza, Accordo/Regolamento interno) possono essere sottoscritti SOLO da chi è intestatario di formale procura che definisce, fra l'altro, eventuali limiti economici relativi all'importo "firmabile".

2.6.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
04 – 01	Nei rapporti con Clienti e, più precisamente, con Funzionari o Rappresentanti della Pubblica Amministrazione (Stato, Ente pubblico o Ente Comunitario), omaggi o benefici materiali sono ammessi (eventualmente a favore di persone a loro vicine) solo ed esclusivamente se tali elargizioni rientrano nelle *normali prassi commerciali* e, cioè, se soddisfano entrambe le seguenti condizioni: A) l'omaggio (o beneficio) è di modico valore; B) l'omaggio (o beneficio) non è tale da poter apparire come: → capace di condizionare l'autonomia di giudizio del beneficiario ovvero → finalizzato ad incoraggiare o a ricompensare l'illecito comportamento del beneficiario in entrambi i casi, *a vantaggio di una Società del Gruppo Engineering*. A chiunque si presenti in nome o per conto di una Società del Gruppo è quindi vietato offrire o promettere a Funzionari o a Rappresentanti della Pubblica Amministrazione (Stato, Ente pubblico o Ente Comunitario) omaggi (o benefici) non rientranti nelle *normali prassi commerciali*. Chiunque riceva, da parte di Terzi, l'offerta o la sollecitazione di un omaggio o di un beneficio che non rientri nelle normali prassi commerciali, è tenuto ad informare il proprio Responsabile diretto ed a darne formale comunicazione alla Direzione Processi e Audit Interno ed all'Organismo di Vigilanza.	**- PGA02 Gestione Ciclo Passivo**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
04 – 02	Data: → la potenziale estensione dei rapporti di relazione fra soggetti ipoteticamente coinvolti in un comportamento corruttivo, → la molteplicità di forme con cui può realizzarsi la dazione di un compenso economico a fronte di illeciti vantaggi richiesti, promessi o conseguiti allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai processi sensibili rientranti nelle procedure di seguito elencate: → Gestione Ciclo Passivo: acquisti ed approvvigionamenti, in particolare: tracciabilità dei flussi finanziari (L. 136/10) in presenza di Cliente finale appartenente alla Pubblica Amministrazione o Concessionario di finanziamenti pubblici → Gestione Richiesta di Acquisizione di Consulenze Informatiche → Gestione Cassa: pagamenti e rendicontazione → Gestione Servizi Finanziari e di Tesoreria: gestione conti correnti bancari → Gestione Risorse Umane: assunzione e gestione del Personale → Gestione Amministrativa RTI/ATI → Gestione Preventivo Fornitura → Gestione Ciclo Attivo: gestione vendite. In linea generale, deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Va sottoposta a gestione centrale controllata la tabella contenente i nomi dei Responsabili intestatari di delega all'autorizzazione delle richiesta d'acquisto, tabella utilizzata dalla procedura informatica che gestisce il ciclo autorizzativo. Analoga gestione controllata e centralizzata va adottata per la tabella contenente i nomi dei Responsabili che possono autorizzare l'emissione di un'Offerta/Contratto di vendita. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**- PGA10 Gestione Contributi per la Ricerca** **- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- PGA04 Gestione Preventivo Fornitura** **- PGA05 Gestione Cassa** **- RS03P02 Procedura Avvio Chiusura Attività** **- RS03P03 Procedura Esecuzione Controllo Attività** **- RS02P01 Procedura Gestione Offerta Prima Qualificazione Fornitori** **- RS02P02 Procedura Gestione Fornitori** **- PGP09 Gestione Risorse Umane** **- PGA06 Gestione Servizi Finanziari e di Tesoreria** **- PGA13 Gestione Amministrativa RTI ATI** **- PGA15 Gestione Richieste Acquisizione Consulenze Informatiche**
04 – 03	Le sottoscrizioni, da parte di un Rappresentante della Società: - di un'Offerta, di una *Risposta ad un bando di gara* o di un Contratto, verso un Cliente (ciclo attivo), ovvero - di un Contratto o di un Ordine, verso un Fornitore (ciclo passivo) sono atti formali che impegnano l'Azienda verso l'esterno; in quanto tali, non possono essere effettuati se non da chi è intestatario di apposita procura scritta, che definisce, fra l'altro, eventuali limiti economici relativi all'importo "firmabile". La titolarità di procure non esime il detentore delle stesse dal rispetto degli adempimenti aziendali prescritti per quanto concerne il processo autorizzativo interno.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
04 – 04	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore la procedura "Gestione Procure/Deleghe" che fissa le norme per il conferimento e l'impiego di procure e deleghe utilizzate nel processo di formalizzazione contrattuale. In particolare, le deleghe possono essere rilasciate dai Procuratori Commerciali entro i limiti della propria procura e sotto la propria responsabilità, solo ed esclusivamente nell'ambito del Ciclo Attivo e per operare con soggetti privati. All'atto del conferimento di una delega devono, in ogni caso, essere rispettati i limiti di valore – dipendenti dal ruolo aziendale del soggetto delegato - così come definiti in apposita tabella pubblicata nella intranet aziendale. Nella stessa rete intranet è reperibile il modello che deve essere obbligatoriamente impiegato per la formalizzazione di una delega.	**- PGA14 Gestione Procure Deleghe**

2.7 Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis del D.Lgs. 231/01)

2.7.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-bis del Decreto richiama specificatamente i seguenti reati.

- Falsificazione di monete, spendita e introduzione nello Stato di monete falsificate, alterazione di monete
- Spendita di monete falsificate ricevute in buona fede
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati, contraffazione di carta filigranata, fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata
- Uso di valori di bollo contraffatti o alterati
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni
- Introduzione nello Stato e commercio di prodotti con segni falsi

Si ritiene qui sufficiente ([2]) limitarsi all'esemplificazione dei soli ultimi due reati richiamati.

- Si contraffanno o si alterano o si fa uso di marchi o di segni distintivi, nazionali o esteri, delle opere dell'ingegno o dei prodotti industriali, ovvero si contraffanno o si alterano o si fa uso di brevetti, di disegni o di modelli industriali, nazionali o esteri
- Si introducono nel territorio dello Stato per farne commercio, si detengono o si pongono in vendita, o si mettono altrimenti in circolazione opere dell'ingegno o prodotti industriali, con marchi o segni distintivi, nazionali o esteri, contraffatti o alterati.

2.7.2 Contestualizzazione aziendale e modalità di commissione

Soggetti/UU.OO. sensibili:

- Dir. Gen. Amm. Fin. e Controllo

([2]) Vedasi, infatti, quanto affermato al successivo paragrafo, in "*Modalità di commissione del reato*".

- Tutte le UU.OO. operanti in ambito tecnico o commerciale

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Gestione Cassa
- Ciclo Attivo (vendite)

Modalità di commissione del reato. La commissione dei primi quattro reati specificatamente richiamati dal presente articolo 25-bis del D.Lgs 231/01 richiederebbe, come condizione in grado di configurare un significativo interesse o vantaggio dell'Azienda (presupposto per l'imputazione dei reati ex D.Lgs 231/01), l'impiego diffuso e consistente, in termini di controvalore, di strumenti come quelli richiamati dai reati-presupposto. Tale impiego risulta, nella prassi aziendale, estremamente limitato, tanto da poter concludere che la commissione dei reati considerati risulta, ancorché *astrattamente*, difficilmente ipotizzabile.

Per quanto concerne la commissione dei reati di falsità in strumenti o segni di riconoscimento, la situazione potrebbe concretizzarsi quando l'Azienda mettesse in vendita prodotti contraddistinti con marchi (o loghi) uguali o simili a quelli di un'altra Società (diversa da un'Azienda del Gruppo). Si allude qui ad una particolare tipologia di fornitura, quella di apparecchiature HW: volendo far riferimento a tale specifica casistica, si può concludere che il volume del fatturato specifico e la marginalità lucrabile sarebbero così poco significativi da rendere (al di là di ogni imprescindibile valutazione etica) "*non pagante*" l'eventuale compimento del reato.

2.7.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.7.3.1 Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2.

2.7.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
05 - 01	Particolare rigore va anche posto nell'applicazione dei protocolli e dei controlli previsti dalle Procedure: → Gestione Cassa → Gestione Ciclo attivo Deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti di vendita debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili.	**- PGA03 Gestione Ciclo Attivo** **- PGA05 Gestione Cassa**

2.8 Delitti contro l'industria e il commercio (Art. 25-bis.1 del D.Lgs. 231/01)

2.8.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-bis.1 del Decreto richiama specificatamente i seguenti reati.

A) - Turbata libertà dell'industria o del commercio

B) - Illecita concorrenza con minaccia o violenza

C) - Frodi contro le industrie nazionali

D) - Frode nell'esercizio del commercio

E) - Vendita di sostanze alimentari non genuine come genuine

F) - Vendita di prodotti industriali con segni mendaci

G) - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale

H) - Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari

Esemplificazioni delle fattispecie di reato richiamate sono, rispettivamente, le seguenti.

A) - Facendo violenza sulle cose o con mezzi fraudolenti si impedisce o si turba l'esercizio di un'industria

B) - Nell'esercizio di un'attività si compiono atti di concorrenza con violenza o minaccia

C) - Si vendono o si mettono in circolazione prodotti con nomi, marchi o segni distintivi contraffatti o alterati, cagionando un nocumento all'industria nazionale

D) - Nell'esercizio di un'attività si consegna all'acquirente una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita

E) - Si pone in vendita o si mettono in commercio come genuine sostanze alimentari non genuine

F) - Si pone in vendita o si mettono in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto

G) - Potendo conoscere dell'esistenza del titolo di proprietà industriale, si fabbricano o si adoperano industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso. Ovvero, al fine di trarne profitto e con riferimento agli stessi beni, questi vengono introdotti nel territorio dello Stato o posti in vendita o comunque in circolazione

H) - Si contraffanno o comunque si alterano indicazioni geografiche o denominazioni di origine di prodotti agroalimentari. Ovvero, al fine di trarne profitto e con riferimento agli stessi prodotti con indicazioni/denominazioni contraffatte, questi vengono introdotti nel territorio dello Stato o posti in vendita o comunque in circolazione.

2.8.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Direzioni commerciali
- Direzioni tecniche di produzione

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Ciclo Attivo (vendite)
- Ciclo Passivo (acquisti ed approvvigionamenti)
- Gestione commessa/Realizzazione di un progetto (interno o esterno)-Erogazione di una fornitura a Cliente

Modalità di commissione del reato.

Con riferimento ai reati precedentemente elencati, di cui alle lettere A) e B): nelle fasi di predisposizione/presentazione di un'Offerta o di una Risposta a Bando di Gara un responsabile commerciale esercita su un concorrente (eventualmente "potenziale") violenze o minacce.

Con riferimento ai reati precedentemente elencati, di cui alle lettere C), D), E) ed H): nella realtà aziendale tali reati non sono neppure astrattamente ipotizzabili.

Per il reato di cui alla lettera F) del precedente elenco: si rimanda a quanto detto, con riferimento all'art. 25-bis del D.Lgs 213/01, a proposito del compimento dei reati di "falsità in strumenti o segni di riconoscimento"

Per il reato di cui alla lettera G) del precedente elenco: con riferimento ad un bene o ad un prodotto sul quale un Terzo vanta un titolo di proprietà industriale, illecitamente (ovvero senza aver preventivamente acquisito un'idonea licenza d'uso) l'Azienda adotta uno dei seguenti comportamenti:

- il bene/prodotto viene strumentalmente utilizzato per finalità interne non direttamente connesse alla vendita di propri prodotti;
- il bene/prodotto di Terzi viene strumentalmente utilizzato nella realizzazione di un proprio prodotto destinato alla vendita ovvero viene direttamente integrato in un prodotto destinato alla vendita.

2.8.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.8.3.1 Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento*" indicati nel paragrafo 2.2.

2.8.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
06 - 01	Con specifico riferimento al reato di cui alla lettera G) del precedente elenco ed, in particolare, all'ipotetica fornitura che incorpora un prodotto di Terzi, devono risultare regolarmente documentati ed autorizzati: - la Richiesta d'Acquisto relativa alla prescritta licenza d'uso - il Preventivo fornitura nel quale figura una specifica voce di costo inerente la licenza. Per entrambi i documenti il processo di autorizzazione deve vedere coinvolti almeno due Responsabili.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- PGA04 Gestione Preventivo Fornitura**

2.9 Reati societari (Art. 25-ter del D.Lgs. 231/01)

2.9.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-ter del Decreto richiama specificatamente i seguenti reati.

- False comunicazioni sociali (art. 2621 c.c.)
- False comunicazioni sociali previsto dall'art. 2621-bis c.c.

- Impedito controllo, indebita restituzione di conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori
- Formazione fittizia del capitale, indebita ripartizione dei beni sociali da parte dei liquidatori

  Illecita influenza sull'assemblea, aggiotaggio,
- Corruzione tra privati
- Istigazione alla corruzione tra privati

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

- Con l'intenzione di ingannare i Soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali si espongono fatti non veri o si omettono informazioni sulla situazione economica, patrimoniale o finanziaria, in modo da indurre in errore i destinatari sulla predetta informativa, eventualmente cagionando un danno patrimoniale alla Società, ai Soci o ai Creditori.
- Si impedisce o si ostacola lo svolgimento delle attività di controllo ai Soggetti (Soci o altri Organi sociali) a cui sono state legalmente attribuite.
- Gli Amministratori:
  - illegittimamente, restituiscono (anche simulatamente) i conferimenti ai Soci o li liberano dall'obbligo di eseguirli
  - ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscono riserve che non possono per legge essere distribuite
  - illegittimamente, acquistano o sottoscrivono azioni o quote sociali (oppure azioni o quote emesse dalla società controllante), cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge
  - in violazione delle disposizioni di legge, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.
- Gli Amministratori e i Soci conferenti formano o aumentano fittiziamente il capitale sociale
- I Liquidatori ripartiscono i beni sociali tra i Soci prima di pagare i creditori sociali, cagionando loro un danno
- Con atti simulati o fraudolenti si determina la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto
- Si diffondono notizie false, si pongono in essere operazioni simulate o altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, ovvero idonei ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari
- Nell'interesse della Società, si dà o si promette denaro o altra utilità ad un Soggetto appartenente ad altra Società privata, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

2.9.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è teoricamente *significativo* ed *esteso*, coinvolgendo i seguenti **Soggetti/UU.OO. sensibili**:

- Consiglio di Amministrazione
- Soci
- Dir. Gen. Amm. Fin. e Controllo
- Tutte le UU.OO. operanti in ambito tecnico o commerciale.

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Gestione della Contabilità Generale ed analitica
- Gestione chiusure contabili
- Gestione del Bilancio
- Gestione adempimenti fiscali
- Gestione Servizi Finanziari e di Tesoreria/Gestione movimenti bancari e flussi finanziari
- Gestione Immobilizzazioni/Gestione cespiti e avviamenti
- Gestione Ciclo Passivo/Trattativa commerciale, Verifica ed autorizzazione contratto, Alimentazione contabilità analitica, Gestione fatturazione e mandati di pagamento
- Gestione Ciclo Attivo/Predisposizione Offerta e trattativa commerciale, Verifica ed autorizzazione contratto, Alimentazione contabilità analitica, Gestione fatturazione
- Gestione Commessa/Verifica e autorizzazione preventivi costi-ricavi, Maturazione costi-ricavi
- Gestione Commessa di Ricerca/Rendicontazione, Avanzamento ricavi
- Gestione Cassa/Pagamento, Rendicontazione
- Gestione Risorse Umane
- Gestione Operazioni con Parti correlate
- Gestione Acquisto-Vendita Partecipazioni e Rami d'Azienda
- Gestione Amministrativa RTI-ATI
- Conferimento ed impiego di Procure-Deleghe di valenza esterna

Relativamente alle **modalità di commissione del reato** si rileva che molteplici sono i Soggetti astrattamente in grado di operare per la commissione di questi reati-presupposto, così come molteplici sono, teoricamente, le modalità con cui gli stessi reati potrebbero essere commessi. In tal senso conviene richiamare la previsione di legge secondo la quale la commissione di illeciti di natura societaria determinano la diretta responsabilità dell'impresa se dall'atto doloso, compiuto da Soggetti apicali, sia discesa una qualche utilità per la Società.

Non va tuttavia dimenticato che alcuni reati possono essere commessi da Soggetti non apicali, con piena responsabilità dell'Ente, nel caso in cui il comportamento doloso dei Subordinati sia stato fatto proprio dai Soggetti apicali o reso possibile da un loro negligente controllo.

A titolo esemplificativo (qualunque elenco risulterebbe infatti inevitabilmente parziale), astrattamente si possono ipotizzare, a livello generale, le seguenti possibili modalità di compimento dei reati in questione:

- uno o più Amministratori, in deroga allo spirito ed al contenuto del codice Etico di Gruppo, dagli Stessi approvato, inducono uno o più soggetti ad operare al fine di produrre dati di Bilancio, relazioni o comunicazioni sociali non veritiere;
- uno o più Amministratori, non fornendo una piena e trasparente collaborazione ai Soggetti a cui sono state legalmente attribuite attività di controllo (Soci o altri Organi sociali), inducono gli stessi Soggetti a valutazioni parziali o errate;
- Dirigenti responsabili di UU.OO amministrative, tecniche o commerciali, attuando un livello di controllo inadeguato presso le strutture che a loro rispondono, non rilevano la sistematica produzione di dati contabili errati, con impatto distorcente su specifiche voci di Bilancio (ad es.: accantonamenti, dati del ciclo attivo/passivo inerenti le commesse, ecc.);
- allo scopo ultimo di conseguire un vantaggio per una Società del Gruppo Engineering, anche per interposta persona, si offre, si promette o si dà denaro o altra utilità non dovuti ad un Soggetto operante in altra Società (amministratori, direttori generali, dirigenti preposti alla redazione dei

documenti contabili societari, sindaci e liquidatori di società o di enti privati), inducendolo a venir meno ai propri doveri di correttezza e fedeltà verso la Società per la quale opera;

- nello scenario delineato al punto precedente, si effettuano irregolari compensazioni economiche fra Partner di un RTI/ATI;
- il Direttore commerciale (o un suo sottoposto) corrisponde o promette una somma di denaro o altra utilità al responsabile acquisti di una società cliente al fine di favorire i prodotti aziendali rispetto a quelli di migliore qualità o con migliore rapporto qualità/prezzo di una concorrente;
- un Dipendente del Gruppo Engineering corrisponde o promette una somma di denaro o altra utilità all'amministratore delegato o al direttore generale di una società concorrente affinché questi ignori una opportunità commerciale rispetto alla quale l'impresa per cui il corruttore lavora ha un proprio interesse;
- il Responsabile della funzione Tecnica Innovazione e Ricerca corrisponde o promette una somma di denaro o altra utilità al Responsabile della medesima funzione di una Società concorrente al fine di farsi rivelare segreti industriali quali informazioni segrete o invenzioni non ancora brevettate.

2.9.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.9.3.1 Principi specifici di comportamento

- E' severamente vietato a chiunque si presenti in nome o per conto di una Società del Gruppo Engineering, offrire, promettere o dare, anche per interposta persona, denaro o altra utilità non dovuti ad un Soggetto operante in altra Società, o enti privati inducendolo così a venir meno ai doveri di correttezza e fedeltà verso la Società per la quale opera, tutto ciò allo scopo ultimo di conseguire un vantaggio per una Società del Gruppo.
- Durante la fase che precede l'emissione di un bando di gara ed in quella di partecipazione alla stessa, il personale di una Società del Gruppo Engineering che, con ruoli di responsabilità, è coinvolto, in qualsiasi forma, in attività commerciali e/o consulenziali verso l'Ente committente, è tenuto a redigere ed aggiornare mensilmente un report nel quale registra, in forma sintetica, tutti i contatti avuti con Responsabili dell'Ente, anche di tipo informale, riportando (oltre alle ovvie circostanze di data, orario, luogo e persone presenti), i contenuti e gli eventuali esiti di tali contatti. Tali evidenze andranno opportunamente conservate, da parte di ciascun Redattore, per essere rese disponibili a richiesta della Direzione Processi e Audit Interno o dell'Organismo di Vigilanza.
- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
  - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.
- Nel caso di fornitura resa all'Ente committente da un RTI/ATI a cui partecipa una Società del Gruppo Engineering, è severamente vietato attuare tra i Partner compensazioni economiche in forma tacita.

Eventuali compensazioni economiche, in qualsiasi forma esse si attuino, dovranno avere forma esplicita, motivata e debitamente formalizzata.

- Allo scopo di avere totale garanzia che nell'ambito del processo di selezione e assunzione del Personale, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), nel contesto del processo di valutazione del Candidato, vanno obbligatoriamente sottoscritte due distinte dichiarazioni, una del Candidato stesso, l'altra del Responsabile aziendale che lo ha sottoposto a colloquio di valutazione, dichiarazioni con le quali tali Soggetti, ciascuno sulla base delle informazioni a sua disposizione, attestano che il processo s'è svolto in assenza di illecite interferenze da parte di Terzi o per illecite finalità.
- Gli Amministratori, l'Alta Direzione aziendale ed, in particolare, il Dirigente preposto alla redazione dei documenti contabili societari, il Responsabile dell'Audit interno e tutte le strutture di cui tali Dirigenti sono responsabili sono tenuti ad un comportamento di massima collaborazione nei confronti dei Soggetti a cui sono state legalmente attribuite attività di controllo (Soci o altri Organi sociali), fornendo loro informazioni vere, chiare, complete e tempestive.
- A chiunque è vietato offrire danaro o altri beni a singoli membri del Collegio Sindacale o a Rappresentanti della Società di Revisione al fine di ottenere un loro atteggiamento connivente;
- La Dir. Gen. Amm. Fin. e Controllo deve comunicare all'Organismo di Vigilanza, con adeguata motivazione, l'eventuale verificarsi, al di fuori delle previste scadenze contrattuali, di uno dei seguenti eventi: revoca di incarico alla Società di Revisione; assegnazione di incarico ad una nuova Società di Revisione;
- Gli atti formali di costituzione di un RTI/ATI (Costituzione RTI/ATI, Mandato speciale di rappresentanza, Accordo/Regolamento interno) possono essere sottoscritti SOLO da chi è intestatario di formale procura che definisce, fra l'altro, eventuali limiti economici relativi all'importo "firmabile".
- A chiunque si trovasse impegnato, per conto di una Società del Gruppo Engineering, nella partecipazione ad una gara o nell'erogazione di una fornitura, è severamente vietato offrire, promettere o dare, anche per interposta persona, denaro o altra utilità non dovuti ad un Soggetto operante in altra Società, o enti privati.

2.9.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
07 - 01	Nelle Società del Gruppo Engineering, ai fini dell'elaborazione e della rappresentazione dei bilanci, delle relazioni, dei prospetti o di altre comunicazioni sociali è vietato a chiunque comunicare o utilizzare informazioni o dati non veritieri, lacunosi e tali comunque da non consentire la rappresentazione della reale situazione economica, patrimoniale e finanziaria della Società.	**- PGA08 Gestione Chiusure Contabili**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
07 - 02	Dati: → l'elevato numero di Dipendenti che, a vari livelli di responsabilità, sono coinvolti nella produzione e nella comunicazione dei dati di Bilancio, → la molteplicità dei processi aziendali che generano dati che confluiscono nei flussi che alimentano le voci contabili e, quindi, il Bilancio allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai *processi sensibili* rientranti nelle procedure di seguito elencate: → Gestione della Contabilità generale ed analitica: aggiornamento del piano dei conti, movimentazioni dirette → Gestione delle Chiusure contabili: analisi scostamenti rispetto ai periodi precedenti e quadrature → Gestione Servizi Finanziari e di Tesoreria/Gestione movimenti bancari e flussi finanziari → Gestione Immobilizzazioni: gestione cespiti e avviamenti → Gestione Ciclo Passivo: verifica preventivi ed autorizzazione contratto, maturazione costi, gestione fatturazione e mandati di pagamento → Gestione Ciclo Attivo: verifica ed autorizzazione preventivo e contratto, maturazione ricavi, gestione fatturazione → Gestione Contributi per la Ricerca: rendicontazioni e maturazione ricavi → Gestione Cassa: pagamento, rendicontazione → Gestione Risorse Umane → Gestione Acquisto/Vendita Partecipazioni e Rami d'Azienda → Gestione Amministrativa RTI/ATI → Gestione Procure/Deleghe. Oltre alla puntuale applicazione del sistema aziendale di deleghe nei processi autorizzativi svolti a monte dell'approvazione del Bilancio consolidato, nello svolgimento dei processi citati va inoltre assicurato che le informazioni generate e comunicate a valle di detti processi siano: → corrette e complete, → supportate da un adeguato livello di documentazione, con archiviazione *a storico* delle registrazioni principali. Infine deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un *processo sensibile*.	**- PGA10 Gestione Contributi per la Ricerca** **- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- PGA04 Gestione Preventivo Fornitura** **- PGA05 Gestione Cassa** **- RS03P02 Procedura Avvio Chiusura Attività** **- RS03P03 Procedura Esecuzione Controllo Attività** **- RS01P01 Procedura Gestione Acquisizione Contratti** **- RS02P02 Procedura Gestione Fornitori** **- PGP09 Gestione Risorse Umane** **- PGP17 Gestione Amministrativa Personale** **- PGA08 Gestione Chiusure Contabili** **- PGA06 Gestione Servizi Finanziari e di Tesoreria** **- PGA07 Gestione Immobilizzazioni** **- PGA11 Gestione Acquisto Vendita Partecipazioni Rami Azienda** **- PGA13 Gestione Amministrativa RTI ATI** **- PGA15 Gestione Richieste Acquisizione Consulenze Informatiche** **- LGA01 Linee Guida per dismissione cespiti**
07- 03	Una specifica Procedura, approvata dal CdA della Capogruppo, fissa precise norme da rispettare nei processi di individuazione, approvazione ed esecuzione di *Operazioni con Parti Correlate*, tali da garantire la trasparenza e la correttezza, sostanziale e procedurale, di tali operazioni, sia se realizzate direttamente che per il tramite di Società controllate. La Procedura si applica, ove compatibile, anche alle Operazioni con Parti Correlate di cui siano parti Società controllate, direttamente o indirettamente, dalla Capogruppo. Il CdA di quest'ultima esamina preventivamente tali operazioni. A questo fine, le Società controllate informano tempestivamente la Capogruppo delle Operazioni con Parti Correlate che intendono approvare, trasmettendo le informazioni e la documentazione necessaria per dare corso a quanto previsto dalla citata Procedura.	**- PROCEDURA PER L'INDIVIDUAZIONE E L'EFFETTUAZIONE DI OPERAZIONI CON PARTI CORRELATE**

2.10 Delitti con finalità di terrorismo o di eversione dell'ordine democratico (Art. 25-quater del D.Lgs. 231/01)

2.10.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-quater del Decreto non richiama specificatamente una serie di reati, bensì fa un generico riferimento ai "*Delitti con finalità di terrorismo o di eversione dell'ordine democratico*" previsti dal codice penale e dalle leggi speciali, nonché all'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999.

2.10.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Dir. Gen. Amm. Fin. e Controllo
- Direzioni tecniche di produzione
- Direzioni commerciali.

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Gestione Anagrafica Fornitori (qualificazione e censimento nuovi Fornitori/modifica dati anagrafici o riferimenti bancari)
- Selezione Fornitori da Albo Fornitori qualificati
- Gestione Ciclo passivo/Valutazione Offerte-Preventivi da Fornitori, Autorizzazione alla spesa, Analisi e sottoscrizione contratto
- Gestione Fatturazione passiva e Mandati di pagamento
- Valutazione Fornitori qualificati ed aggiornamento Albo
- Gestione Ciclo attivo/Verifica e autorizzazione preventivi costi-ricavi, Analisi e sottoscrizione contratto, Maturazione costi-ricavi
- Gestione Fatturazione attiva
- Gestione Anagrafica Clienti (censimento nuovi Clienti/modifica dati anagrafici)

Relativamente alla **modalità di commissione del reato** si può astrattamente ipotizzare un interesse od un vantaggio della Società (condizione presupposto per l'imputabilità di un reato ex D.Lgs. 231/01), a fronte di rapporti instaurati con Fornitori o con Clienti operanti con finalità di terrorismo o di eversione dell'ordine democratico, laddove i citati rapporti fossero in grado di soddisfare, reciprocamente, gli interessi della Società e quelli dell'organizzazione terroristica o eversiva.

2.10.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.10.3.1 Principi specifici di comportamento

Si rimanda ai "Principi generali di comportamento" indicati nel paragrafo 2.2.

2.10.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
08 - 01	Allo scopo di ridurre al minimo il rischio di compimento del reato qui considerato, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai *processi sensibili* rientranti nelle procedure di seguito elencate: → Gestione Anagrafica Fornitori: qualificazione e censimento nuovi Fornitori/modifica dati anagrafici e riferimenti bancari → Gestione Albo Fornitori qualificati: selezione Fornitori da Albo, valutazione Fornitori qualificati ed aggiornamento Albo → Gestione Ciclo passivo: valutazione Offerte-Preventivi da Fornitori, autorizzazione alla spesa, analisi e sottoscrizione contratto, gestione fatturazione passiva e mandati di pagamento → Gestione Ciclo attivo: verifica e autorizzazione preventivi costi-ricavi, analisi e sottoscrizione contratto, maturazione costi-ricavi, gestione fatturazione attiva → Gestione Anagrafica Clienti: censimento nuovi Clienti/modifica dati anagrafici Deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Entrambi i tipi di contratto devono essere firmati da chi è dotato di apposita specifica Procura, così come documentato nel sistema di Procure gestito, sotto controllo, a livello centrale. Va sottoposta a gestione centrale controllata anche la tabella contenente i nomi dei Responsabili intestatari di delega all'autorizzazione delle richiesta d'acquisto, tabella utilizzata dalla procedura informatica che gestisce il ciclo autorizzativo. Analoga gestione controllata e centralizzata va adottata per la tabella contenente i nomi dei Responsabili che possono autorizzare l'emissione di un'Offerta/ Contratto di vendita. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- PGA04 Gestione Preventivo Fornitura** **- RS03P03 Procedura Esecuzione Controllo Attività** **- RS01P01 Procedura Gestione Acquisizione Contratti** **- RS02P01 Procedura Gestione Offerta Prima Qualificazione Fornitori** **- RS02P02 Procedura Gestione Fornitori**

2.11 Delitti contro la personalità individuale (Art. 25-quinquies del D.Lgs. 231/01)

2.11.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-quinquies del Decreto richiama specificatamente i seguenti reati.

- Riduzione o mantenimento in schiavitù o in servitù
- Prostituzione minorile, pornografia minorile, detenzione di materiale pornografico
- Pornografia virtuale
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile
- Tratta di persone, acquisto e alienazione di schiavi
- Intermediazione illecita e sfruttamento del lavoro

Esemplificazione delle fattispecie di reato sopra elencate:

nel presente paragrafo, si fornirà l'analisi e la descrizione del reato di Intermediazione illecita e sfruttamento del lavoro di cui all'art. 603-*bis* c.p..

Per quanto riguarda tutti gli altri reati richiamati dall'art. 25-*quinquies* del D.Lgs. 231/01, la loro commissione implicherebbe lo svolgimento di attività che non risultano neppure astrattamente ipotizzabili in ambito aziendale e che, comunque, non soddisfarebbero la condizione di realizzare un interesse o un vantaggio dell'Ente..

Il reato di cui all'art. 603-*bis* c.p., recentemente modificato dalla Legge 29 ottobre 2016, n. 199 (entrata in vigore il 4 novembre 2016) punisce, salvo che il fatto costituisca più grave reato, "*chiunque: 1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori; 2) 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*".
Se i fatti sono commessi "*mediante violenza o minaccia*" si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.
La norma prevede, al quarto comma, delle aggravanti ad effetto speciale che comportano l'aumento della pena da un terzo alla metà: 1) se il numero di lavoratori reclutati è superiore a tre; 2) se uno o più dei soggetti reclutati sono minori in età non lavorativa; 3) se il fatto è stato commesso esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

Si tratta di una fattispecie punita a titolo di dolo; pertanto, ai fini dell'integrazione del reato, le condotte rilevano solo ove sorrette dalla consapevolezza e dalla volontà di sottoporre "*i lavoratori a condizioni di sfruttamento*" approfittando "*del loro stato di bisogno*".

2.11.2 Contestualizzazione aziendale e modalità di commissione

Per quanto riguarda il reato di "*Intermediazione illecita e sfruttamento del lavoro*", l'esposizione al rischio di Engineering riguarda le seguenti **Direzioni Generali**:

- Dir. Gen. Human Resource & Organization
- Servizio Salute & Sicurezza e Ambiente
- Direzione Generale Amministrazione Finanza e Controllo

Inoltre, l'esposizione al rischio di realizzazione del reato in esame, cui è esposto la Società, riguarda le seguenti **UU.OO:**

- Direzione Amministrazione del Personale
- Direzione Risorse umane Area Nord
- Direzione Risorse umane Area Centro Sud
- Servizio Salute Sicurezza e Ambiente
- Direzione Acquisti e Affari Generali

I **processi/sottoprocessi sensibili** al rischio sono i seguenti:

- gestione del rapporto di collaborazione con un dipendente o con un lavoratore autonomo nella fase della instaurazione e durante l'esecuzione dello stesso;
- scelta e gestione del rapporto con fornitori, appaltatori, partner in relazione all'applicazione ed al rispetto del D. Lgs. 81/08 in materia di salute e sicurezza sul lavoro;

- rapporti con soggetti terzi che implicano l'utilizzo da parte dell'Ente di manodopera facente capo ai medesimi soggetti terzi.

Relativamente alle **modalità di commissione del reato**, la fattispecie di "***Intermediazione illecita e sfruttamento del lavoro***", a titolo meramente esemplificativo, potrebbe realizzarsi nelle ipotesi in cui la Società occupasse alle proprie dipendenze dei lavoratori, sottoponendoli a condizioni di sfruttamento secondo gli "indici" di cui al terzo comma dell'art. 603-*bis* c.p. e, più precisamente, secondo l'elencazione contenuta nella norma:

- corrispondendo ai lavoratori, in modo reiterato, retribuzioni che siano palesemente difformi rispetto alle indicazioni contenute nei contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale e concretamente applicabili;

- corrispondendo ai lavoratori, in modo reiterato, una retribuzione che sia comunque sproporzionata rispetto alla quantità e alla qualità del lavoro prestato;

- violando, in modo reiterato, la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria e alle ferie;

- violando le norme in materia di sicurezza e di igiene nei luoghi di lavoro di cui al D. Lgs. 81/08 e le prescrizioni contenute nel *Sistema di Gestione della salute e Sicurezza dei Lavoratori* (*SGSL*) adottato dall'Azienda;

- sottoponendo il lavoratore a condizioni di lavoro, metodi di sorveglianza o a situazioni alloggiative degradanti.

Preme precisare che qualora le condotte di Intermediazione illecita e sfruttamento del lavoro siano poste in essere nei confronti di lavoratori stranieri privi di valido permesso di soggiorno, la fattispecie in esame concorrerebbe con il reato di "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*" di cui all'art. 25-*duodecies* del Decreto. Trattandosi di fattispecie entrambe previste quali reati presupposto della responsabilità ex D. Lgs. 231/2001, la loro contestuale realizzazione darebbe vita, infatti, a distinti illeciti a carico dell'Ente.

2.11.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.11.3.1 Principi specifici di comportamento

Preme osservare come il reato di Intermediazione illecita e sfruttamento del lavoro, nella sua attuale formulazione, punisce tanto le ipotesi (i) di reclutamento diretto della manodopera, da parte della Società, allo scopo di destinarla al lavoro presso terzi in condizione di sfruttamento e approfittando del loro stato di bisogno (cfr. art. 603-*bis*, comma 1, n. 1 c.p.), quanto le ipotesi (ii) di utilizzo, assunzione, impiego di lavoratori anche **tramite attività di intermediazione svolta da terzi** (art. 603-*bis*, comma 1, n. 2 c.p.).

Con riferimento alle ipotesi di cui al superiore punto (i) si indicano di seguito i principi specifici di comportamento attuati dalla Società, al fine di prevenire la commissione del reato.

Le funzioni aziendali competenti :

- in sede di instaurazione del rapporto di lavoro dipendente devono garantire la corresponsione ai lavoratori di una retribuzione conforme alle disposizioni contenute nei CCNL applicabili e, comunque, proporzionata rispetto alla qualità e alla quantità del lavoro prestato;
- devono dare puntuale esecuzione agli obblighi retributivi derivanti dai contratti;
- devono adeguare puntualmente le previsioni contrattuali relative alla retribuzione alle eventuali modifiche dei CCNL applicabili;

- devono adeguare la programmazione degli orari di lavoro, del riposo settimanale, dell'aspettativa obbligatoria e delle ferie di ciascun lavoratore alle prescrizioni contenute nei CCNL concretamente applicabili; devono vigilare affinché i lavoratori non siano sottoposti a condizioni di lavoro, metodi di sorveglianza o a situazioni alloggiative degradanti.

Considerata la rilevanza, anche per quanto di interesse in questa sede, delle misure in materia di sicurezza e igiene nei luoghi di lavoro, al fine della riduzione dei rischi di verificazione del reato di intermediazione illecita e sfruttamento del lavoro, i Destinatari sono tenuti alla scrupolosa osservanza dei principi di comportamento contenuti nella Sezione Speciale del Modello dedicata ai reati di Omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Si precisa che la violazione delle norme in materia di sicurezza e di igiene sul lavoro rileva ai fini della integrazione del reato di cui all'art. 603-*bis* c.p. a prescindere dall'effettivo verificarsi di un infortunio e/o dall'esposizione del lavoratore a pericolo per la salute, la sicurezza o l'incolumità personale.

Con riferimento alle ipotesi di cui al superiore punto (ii) si indicano di seguito i principi specifici di comportamento attuati dalla Società, al fine di prevenire la commissione del reato.

Le funzioni aziendali competenti:

- devono selezionare prestatori di servizi o forniture che si avvalgono di manodopera assunta mediante procedure tali da garantire il rispetto della normativa vigente in ambito sindacale e degli adempimenti imposti dalla contrattazione collettiva, nonché delle norme in materia di salute e sicurezza sul lavoro;
- devono curare che venga previsto l'inserimento nei che prevedano l'impiego, diretto/indiretto, in qualsiasi forma da parte di Engineering di manodopera fornita da tali ultimi soggetti, di specifiche clausole con cui la controparte dichiari, sotto propria responsabilità, di agire nel rispetto delle normative vigenti in ambito sindacale e, quindi, di osservare, nella gestione del personale alle proprie dipendenze, le norme in materia di trattamento retributivo, orario di lavoro, riposo settimanale, ferie, ecc., nonché delle norme in materia di salute e sicurezza sul lavoro;
- devono curare che venga previsto l'inserimento nei contratti che prevedano l'impiego diretto e/o indiretto, in qualsiasi forma, da parte di Engineering di manodopera fornita da tali ultimi soggetti, di specifiche clausole che prevedano la risoluzione del contratto nel caso di violazione, da parte del contraente, delle norme indicate al punto precedente.

2.11.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
09-01	In ottemperanza al D.Lgs. 81/08 in tema di *tutela della salute e della sicurezza nei luoghi di lavoro*, la Società integra il presente Modello con un sistema normativo, il *Sistema di Gestione della salute e Sicurezza sul Lavoro* ("SGSL"), che prevede specifici obblighi giuridici, specifici protocolli e procedure. Il Sistema *SGSL* viene descritto in un *Manuale* che, oltre a riportare le norme di gestione del Sistema, deve prevedere, fra l'altro: - l'obbligatorietà della sua osservanza da parte di chiunque operi nella Società (Vertice aziendale e Dipendenti); - l'impegno a diffondere la cultura della Sicurezza in tutti gli ambiti della vita aziendale, interni ed esterni, promuovendo anche la creazione di apposite strutture destinate a valutare ed, eventualmente,	**- MGSL - Manuale Sistema di Gestione della Sicurezza dei Lavoratori**

	a sanzionare comportamenti che violino le norme applicabili.	
09-02	In tutti i casi in cui si configura un appalto sia in qualità di Committente sia con il ruolo di Fornitore, l'Azienda garantisce la conformità a quanto previsto dall'art. 26 del D.Lgs.81/2008. Le prescrizioni sono inserite nelle procedure amministrativo gestionali di riferimento (rif. **PGA02_0_Gestione_Ciclo_Passivo**, **PGA03_0_Gestione_Ciclo_Attivo** e relativi allegati).	**- MGSL - Manuale Sistema di Gestione della Sicurezza dei Lavoratori**
09-03	L'azienda stabilisce e mantiene attive le procedure per garantire l'individuazione ed il controllo di potenziali emergenze attraverso piani di intervento che siano in grado di: ▪ rispondere in modo adeguato a situazioni di emergenza e/o a potenziali incidenti; ▪ prevenire ed attenuare le conseguenze derivanti da incidenti e situazioni di emergenza. Per le caratteristiche generali della gestione delle emergenze si rimanda alla procedura **PGS01_0_Gestione_Emergenze**. In conformità alla norma di riferimento, per ciascuna sede è redatto un piano di emergenza (PEE rif. **SPP_*cod.Azienda*_PEE_*cod.Sede***) - diffuso a tutto il personale indipendentemente dalla sede di appartenenza mediante pubblicazione sulla intranet aziendale - il cui scopo è prevenire e mitigare gli effetti di eventi accidentali conseguenti a condizioni anomale che possono causare incidenti, infortuni o impatti sulla salute e sicurezza dei lavoratori e/o di terzi in genere. All'interno del piano di emergenza, sono descritte l'organizzazione e le modalità di gestione delle emergenze ivi comprese incendio e primo soccorso. La prova pratica di evacuazione, effettuata periodicamente come da prescrizioni normative, rappresenta lo strumento attraverso cui l'Azienda intende garantire nel tempo la propria preparazione nei confronti di situazioni di rischi di eventuali incidenti. I piani di emergenza sono soggetti a periodica revisione in sede del riesame del SGSL e comunque dopo il verificarsi di emergenze o nel caso di variazione nei processi aziendali significativi ai fini della sicurezza.	**- MGSL - Manuale Sistema di Gestione della Sicurezza dei Lavoratori**
09-04	Il monitoraggio di 1° livello ha lo scopo di tenere sotto controllo le misure preventive e protettive predisposte dall'azienda in materia di SSL. Il monitoraggio di 1° livello è svolto principalmente da parte dell'operatore e dal preposto che, data la natura delle attività svolte in Azienda , verificano : ▪ che siano attuati i comportamenti attesi (rif. **LGS01_0_Vademecum_Salute_Sicurezza,** procedure – di tipologia varia- messe a punto dall'Azienda, etc.) per attività svolte presso sedi aziendali, ▪ che siano rispettate le prescrizioni fornite dal soggetto ospitante ne nel caso in cui le attività siano svolte presso sedi di soggetti terzi. Se il monitoraggio comporta la verifica di aspetti specialistici (ad esempio per verifiche strumentali) è possibile affidarlo ad altre risorse interne o esterne all'azienda quali MC, personale del SPP, professionisti esterni specializzati. Rientrano in questa tipologia di verifiche i sopralluoghi periodici effettuati	**- MGSL - Manuale Sistema di Gestione della Sicurezza dei Lavoratori**

	dall'RSPP presso le sedi aziendali i cui verbali sono conservati dal SPP stesso.	

2.12 Omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-septies del D.Lgs. 231/01)

2.12.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-septies del Decreto richiama specificatamente i seguenti reati.

- *Omicidio colposo* commesso con violazione dell'art. 55, comma 2, del D.Lgs. 81/08;
- *Lesioni personali colpose* commesso con violazione delle norme in materia di salute e sicurezza sul lavoro

Esemplificazione delle fattispecie di reato richiamate è la seguente.

Per *colpa* (negligenza, imprudenza o imperizia nell'applicazione delle norme di legge) viene commesso un omicidio colposo o una persona subisce lesioni personali gravi o gravissime.

2.12.2 Contestualizzazione aziendale e modalità di commissione

Con questa tipologia di reato per la prima volta nell'ambito del D.Lgs. 231/01 viene introdotta la responsabilità per reati di natura "*colposa*" (caratterizzati dal fatto che l'evento verificatosi *non era voluto* da colui che ha agito). Ciò pone una questione interpretativa, osservando che in tal caso la "*non volontarietà*" che caratterizza tali reati *colposi* (omicidio o lesioni personali gravi o gravissime) va conciliata con il presupposto della responsabilità dell'Ente, ex D.Lgs. 231/01, ovvero con la condizione che dal fatto illecito derivi un vantaggio per l'Ente. Tale conciliazione si realizza laddove si osservi che la mancata adozione di un adeguato *Sistema di Gestione della salute e della Sicurezza sul Lavoro ("*SGSL*")* potrebbe essere interpretato come un "risparmio" in termini, ad esempio, di costi, da parte dell'Ente.

Rispetto ai reati-presupposto qui richiamati ed in considerazione della tipologia di attività svolte abitualmente in Azienda, l'esposizione al rischio della Società non è ritenuta di estrema rilevanza *statistica*, soprattutto se confrontata con quella che caratterizza l'insieme delle aziende a cui la norma di riferimento (il D.Lgs. 81/08 - *Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro*) si applica.

Nondimeno, La Società ha ritenuto di considerare i reati qui trattati come "*reati di particolare rilevanza*" e di sanzionarli con maggior severità nell'ambito del sistema disciplinare descritto nel presente Modello.

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Legale rappresentante o persona nominata dal CdA
- Responsabile Dir. Gen. Human Resource & Organization
- Responsabile del Servizio Salute & Sicurezza e Ambiente
- Responsabile di Unità Organizzativa
- Responsabile della sede aziendale (c.d. "Capo Palazzo").

Si ritiene di non poter evidenziare **processi/sottoprocessi** più di altri **sensibili** rispetto al rischio di commissione dei reati qui considerati.

La **modalità di commissione del reato** che si può ipotizzare è la seguente.

Per *negligenza, imprudenza* o *imperizia*, quindi in assenza della volontà che caratterizza il dolo, ma come conseguenza non voluta del perseguimento di una determinata finalità (quale, ad esempio, il contenimento dei costi), si determina un evento accidentale che porta alla morte di una persona o ne cagiona lesioni gravi o gravissime.

La commissione dei reati qui considerati potrebbe essere resa possibile dall'inosservanza del *Sistema di Gestione della salute e Sicurezza dei Lavoratori* (*SGSL*). Tale Sistema, recepito nel presente Modello come sua parte integrante, è specificamente volto a scongiurare il verificarsi di un evento accidentale come quello a cui s'è appena fatto riferimento. Esso prevede infatti il rispetto di tutti gli obblighi elencati all'art. 30 del D. Lgs. 81/08, primo comma, obblighi relativi:

a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro;

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

2.12.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.12.3.1 Principi specifici di comportamento

- La funzione di Internal Auditing è tenuta a svolgere un controllo di 3° livello rispetto all'adozione ed effettiva attuazione del sistema SGSL e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate

*2.12.3.2 **Protocolli e controlli specifici relativi ai processi aziendali***

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
10 - 01	In ottemperanza al D.Lgs. 81/08 in tema di *tutela della salute e della sicurezza nei luoghi di lavoro*, la Società integra il presente Modello con un sistema normativo, il *Sistema di Gestione della salute e Sicurezza sul Lavoro* ("SGSL"), che prevede specifici obblighi giuridici, specifici protocolli e procedure. Il Sistema *SGSL* viene descritto in un *Manuale* che, oltre a riportare le norme di gestione del Sistema, deve prevedere, fra l'altro: - l'obbligatorietà della sua osservanza da parte di chiunque operi nella Società (Vertice aziendale e Dipendenti); - l'impegno a diffondere la cultura della Sicurezza in tutti gli ambiti della vita aziendale, interni ed esterni, promuovendo anche la creazione di apposite strutture destinate a valutare ed, eventualmente, a sanzionare comportamenti che violino le norme applicabili.	**- MSGSL Manuale Sistema di Gestione della Sicurezza dei Lavoratori**
10 - 02	Il Sistema *SGSL* deve prevedere ed attuare i seguenti protocolli: → rispetto degli obblighi giuridici di cui alle lettere da (a) ad (h) dell'art. 30 del D.Lgs. 81/08, primo comma, relativi: ==> a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici; ==> b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti; ==> c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza; ==> d) alle attività di sorveglianza sanitaria; ==> e) alle attività di informazione e formazione dei lavoratori; ==> f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori; ==> g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge; ==> h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate. → adozione di sistemi di registrazione delle attività svolte; → adozione di un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, la valutazione, la gestione ed il controllo del rischio; → adozione di un sistema di controllo sull'attuazione di quanto da esso prescritto e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.	**- PGA02 Gestione Ciclo Passivo**
10 - 03	Ogniqualvolta, a fronte di un contratto di acquisizione di servizi, il personale del Fornitore abbia la necessità di accedere a locali aziendali o a sedi di nostri Clienti (o comunque *di Terzi*), vanno rigorosamente osservate le norme riportate nelle Procedure Gestione del Ciclo Passivo e Gestione Ciclo Attivo, con particolare riferimento a quelle che richiamano adempimenti ex D.Lgs. 81/2008 riguardante la tutela della salute e della sicurezza nei luoghi di lavoro.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo**

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
10 - 04	Ogniqualvolta, a fronte di un contratto di fornitura, sia previsto che le attività siano svolte, in toto o in parte, presso sedi del Cliente, vanno rigorosamente osservate le norme riportate nelle Procedure Gestione del Ciclo Attivo e Gestione Ciclo Passivo, con particolare riferimento a quelle che richiamano adempimenti ex D.Lgs. 81/2008 riguardante la tutela della salute e della sicurezza nei luoghi di lavoro.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo**

2.13 Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies del D.Lgs. 231/01)

2.13.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-octies del Decreto richiama specificatamente i seguenti reati.

- Ricettazione
- Riciclaggio
- Impiego di denaro, beni o utilità di provenienza illecita
- Autoriciclaggio (fattispecie di reato introdotta dalla legge 15 dicembre 2014, n. 186).

Alcune considerazioni in tema di autoriciclaggio.

Il reato di autoriciclaggio, di cui all'art. 648–ter.1 c.p., introdotto con la Legge n. 186/2014 punisce chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce in attività economiche, finanziarie, imprenditoriali o speculative il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

La nuova fattispecie di autoriciclaggio è stata inserita tra i reati-presupposto della responsabilità dell'ente ai sensi dell'art. 25 octies del D.Lgs. 231/2001 con il chiaro intento del legislatore di neutralizzare gli sviluppi economici del reato compiuto a monte dal reo, evitando che le condotte di riciclaggio o reimpiego dei beni di provenienza illecita possano essere svolte per mezzo o attraverso la copertura di una persona giuridica.

L'incertezza della norma, nonché l'assenza di pronunce giurisprudenziali sul tema, pongono profili problematici in ordine alla identificazione dei limiti di applicazione della nuova fattispecie.

Il problema principale ruota intorno alla mancata identificazione dei c.d. reati–base da cui può avere origine la condotta tipica di autoriciclaggio (l'art. 648 *ter*.1, infatti, si riferisce genericamente ai *"delitti non colposi"*) che si riflette, di conseguenza, sulla difficoltà di circoscrivere i confini della responsabilità amministrativa dell'ente.

All'indomani dall'entrata in vigore della nuova fattispecie, infatti, ci si interroga se la responsabilità dell'ente debba essere limitata alle ipotesi in cui il reato–base dell'autoriciclaggio rientri nell'elenco dei reati – presupposto della responsabilità ai sensi del D.Lgs. 231/2001, o se, viceversa, possa configurarsi anche in presenza di fattispecie diverse, estranee al catalogo dei reati di cui al D.Lgs. 231/2001.

Al riguardo due considerazioni.

In primo luogo, la prima interpretazione (restrittiva) sembrerebbe più coerente con il principio di legalità e tassatività posto alla base della disciplina della responsabilità amministrativa dell'ente, sancito dall'art. 2 del Decreto secondo il quale *"l'ente non può essere ritenuto responsabile per un fatto costituente reato se la sua responsabilità amministrativa in relazione a quel reato e le relative sanzioni non sono espressamente previste da una legge entrata in vigore prima della commissione del fatto".* L'intento del

legislatore, fin dall'adozione originaria del D. Lgs. n. 231/2001, è stato, infatti, quello di configurare la responsabilità amministrativa dell'ente derivante da reati con riferimento ad un catalogo determinato di fattispecie criminose, incrementato di volta in volta attraverso i successivi interventi legislativi.

In secondo luogo, preme evidenziare che laddove si privilegiasse l'interpretazione estensiva, volta a far sorgere la responsabilità dell'ente per autoriciclaggio, qualunque sia il reato–base (potendo, quindi, anche non essere contemplato nell'elenco dei reati presupposto di cui al D.Lgs. 231/2001), sarebbe necessario aggiornare il Modello Organizzativo, ricomprendendovi tutti i delitti non colposi previsti dall'attuale ordinamento, con l'inevitabile ricaduta in termini di inefficacia del Modello stesso. Infatti, tanto maggiore è il numero dei reati la cui realizzazione il Modello mira ad evitare, tanto minore rischia di essere l'efficacia complessiva del Modello stesso, come ribadito dalla circolare n. 19867 di CONFINDUSTRIA ([3]).

Un problema di analoga natura si è posto con riferimento alle fattispecie di reati associativi (inclusi nel catalogo dei reati 231 dall'art. 24-*ter*), anch'essi, a causa della loro struttura "aperta", idonei ad allargare il campo ad altre fattispecie criminose (i c.d. "reati scopo").

Sul punto si dà atto dell'intervento della Corte di Cassazione che ha circoscritto l'operatività dell'art. 24-*ter* nel senso di negare la possibilità di attrarre indirettamente alla responsabilità *ex* 231 i delitti-scopo del reato associativo; a ragionare diversamente, infatti, "*la norma incriminatrice di cui all'art. 416 c.p. si trasformerebbe, in violazione del principio di tassatività del sistema sanzionatorio contemplato dal D.Lgs. n. 231 del 2001, in una disposizione 'aperta', dal contenuto elastico, potenzialmente idoneo a ricomprendere nel novero dei reati-presupposto qualsiasi fattispecie di reato, con il pericolo di un'ingiustificata dilatazione dell'area di potenziale responsabilità dell'ente collettivo, i cui organi direttivi, peraltro, verrebbero in tal modo costretti ad adottare su basi di assoluta incertezza e nella totale assenza di oggettivi criteri di riferimento, i modelli di organizzazione e di gestione previsti dal citato D.Lgs., art. 6, scomparendone, di fatto, ogni efficacia in relazione agli auspicati fini di prevenzione*" (Cassazione penale, Sez. VI, 20 dicembre 2013, n. 3635).

In attesa di riscontri giurisprudenziali che possano essere d'ausilio nel far chiarezza circa i limiti applicativi della nuova fattispecie e alla luce delle indicazioni contenute nella citata Circolare n. 19867 di CONFINDUSTRIA, si è ritenuto ragionevole predisporre un Modello Organizzativo che preveda (rispetto alle aree a rischio di commissione del reato di autoriciclaggio) dei presidi a valle finalizzati a prevenire il delitto di autoriciclaggio e, quindi, volti ad evitare che siano impiegati in attività imprenditoriali, economiche o finanziarie della Società, proventi illeciti derivanti da qualsiasi delitto non colposo (anche se non previsto come reato – presupposto della responsabilità dell'ente), la cui elusione sia sanzionata in via disciplinare dalla Società.

Tali presidi predisposti ad hoc andranno ad aggiungersi, nel caso in cui il reato–base sia, altresì, previsto come reato – presupposto della responsabilità dell'ente, alle cautele già adottate per la prevenzione del reato fonte.

Premesse tali considerazioni, si elencano le seguenti esemplificazioni delle fattispecie di reato richiamate.

- Si acquista, si riceve o si occulta denaro o cose di provenienza illecita.
- Si sostituiscono o si trasferiscono denaro, beni o altre utilità di provenienza illecita, ovvero si compiono, in relazione ad essi, altre operazioni in modo da ostacolare l'identificazione della loro illecita provenienza.
- Si impiegano, in attività economiche o finanziarie, denaro, beni o altre utilità di illecita provenienza.
- Avendo commesso o concorso a commettere un delitto non colposo, si impiega, si sostituisce, si trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre

([3]) In particolare, si legge nella circolare n. 19867 di CONFINDUSTRIA che *"… ipotizzare l'insorgere della responsabilità dell'ente per tutti i reati previsti nel nostro ordinamento, quali reati–base dell'autoriciclaggio, vorrebbe dire sovraccaricare il sistema di prevenzione attivato dall'impresa, vanificandone l'efficacia".*

utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

2.13.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Dir. Gen. Amm. Fin. e Controllo
- Direzioni commerciali
- Direzioni tecniche di produzione

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Operazioni di compravendita di strumenti finanziari
- Operazioni di compravendita inerenti la fornitura di prodotti, beni o servizi
- Ciclo Passivo (acquisti ed approvvigionamenti)/Gestione fatturazione
- Ciclo Attivo (vendite)/Gestione fatturazione
- Gestione Amministrativa RTI-ATI/Gestione rapporti economici fra Partner
- Gestione Acquisto-Vendita Partecipazioni e Rami d'Azienda
- Gestione Operazioni con Parti correlate
- Conferimenti o apporti di capitali in società o altri enti
- Transazioni infragruppo
- Operazioni immobiliari.

La **modalità di commissione del reato** che si può astrattamente ipotizzare è la seguente.

Con riferimento a denaro, beni o altre utilità di provenienza illecita:

- si compiono operazioni di acquisto, ricezione od occultamento;
- si attuano irregolari compensazioni economiche fra Partner di un RTI/ATI;
- si impiegano tali beni in operazioni di tipo economico/finanziario;
- si impiegano tali beni in operazioni di tipo economico/finanziario in modo da ostacolare concretamente l'identificazione della loro illecita provenienza.

2.13.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.13.3.1 Principi specifici di comportamento

- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione

contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;

- l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.

- Nel caso di fornitura resa all'Ente committente da un RTI/ATI a cui partecipa una Società del Gruppo Engineering, è severamente vietato attuare tra i Partner compensazioni economiche in forma tacita. Eventuali compensazioni economiche, in qualsiasi forma esse si attuino, dovranno avere forma esplicita, motivata e debitamente formalizzata.
- Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, con particolare riferimento al reato di autoriciclaggio, la Società:
  - condanna qualunque comportamento volto ad impiegare in proprie attività economiche, finanziarie, imprenditoriali o speculative denaro, beni o altre utilità di provenienza delittuosa;
  - vigila affinché coloro i quali operano nelle aree giudicate a rischio reato rispettino le leggi, regolamenti e le procedure di comportamento stabiliti in materia di gestione delle risorse finanziarie, azionarie e immobiliari, volti ad impedire ogni possibile utilizzo economico di proventi delittuosi;
  - prevede obblighi di segnalazione in ordine ad operazioni "atipiche" di impiego in attività economiche, finanziarie, imprenditoriali e speculative della società.

  Rappresentano indici di atipicità di un'operazione che la rendono meritevole di essere oggetto di specifica valutazione al fine di garantire la legittimità rispetto alle finalità di prevenzione del rischio antiriciclaggio:
  1) l'estraneità o incoerenza con l'oggetto sociale, con l'attività o con il profilo economico – patrimoniale della società o del gruppo a cui la stessa appartiene;
  2) l'assenza di adeguata giustificazione, sotto il profilo della normale attività gestionale e sociale, avuto riguardo alla straordinarietà dell'importo o alle inusuali modalità di realizzazione;
  3) la presenza di controparti commerciali operanti in Paesi con regime antiriciclaggio non equivalente a quello dei Paesi della Comunità Europea.

  In presenza di uno o più indici di atipicità sono previste le seguenti modalità di segnalazione:
  a) in caso di operazioni rientranti nei limiti dei poteri di firma e di spesa di un singolo Responsabile, questi ne informa prontamente il Presidente del CdA e l'OdV per le verifiche necessarie;
  b) se l'operazione atipica è di competenza del CdA, quest'ultimo trasmette, agli stessi fini, all'OdV l'ordine del giorno o la relativa delibera.

  Le predette segnalazioni devono essere formalizzate in apposite schede di evidenza.
- La Società prevede con continuità e tenendo conto della evoluzione normativa in materia di antiriciclaggio, adeguata attività di formazione dei soggetti responsabili di operazioni economiche, finanziarie, imprenditoriali o speculative interessati alle aree a rischio reato sulla corretta individuazione degli elementi di atipicità.

2.13.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
11 – 01	Una specifica Procedura, approvata dal CdA della Capogruppo, fissa precise norme da rispettare nei processi di individuazione, approvazione ed esecuzione di *Operazioni con Parti Correlate*, tali da garantire la trasparenza e la correttezza, sostanziale e procedurale, di tali operazioni, sia se realizzate direttamente che per il tramite di Società controllate. La Procedura si applica, ove compatibile, anche alle Operazioni con Parti Correlate di cui siano parti Società controllate, direttamente o indirettamente, dalla Capogruppo. Il CdA di quest'ultima esamina preventivamente tali operazioni. A questo fine, le Società controllate informano tempestivamente la Capogruppo delle Operazioni con Parti Correlate che intendono approvare, trasmettendo le informazioni e la documentazione necessaria per dare corso a quanto previsto dalla citata Procedura.	**- PROCEDURA PER L'INDIVIDUAZIONE E L'EFFETTUAZIONE DI OPERAZIONI CON PARTI CORRELATE**
11 – 02	Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai *processi sensibili* rientranti nelle procedure di seguito elencate: → Gestione Anagrafica Fornitori: qualificazione e censimento nuovi Fornitori/modifica dati anagrafici e riferimenti bancari → Gestione Albo Fornitori qualificati: selezione Fornitori da Albo, valutazione Fornitori qualificati ed aggiornamento Albo → Gestione Ciclo passivo: autorizzazione alla spesa, analisi e sottoscrizione contratto, gestione fatturazione passiva e mandati di pagamento → Gestione Ciclo attivo: verifica e autorizzazione preventivi costi-ricavi, analisi e sottoscrizione contratto, gestione fatturazione attiva → Gestione Anagrafica Clienti: censimento nuovi Clienti/modifica dati anagrafici → Gestione Acquisto/Vendita Partecipazioni e Rami d'Azienda Deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Entrambi i tipi di contratto devono essere firmati da chi è dotato di apposita specifica Procura, così come documentato nel sistema di Procure gestito, sotto controllo, a livello centrale. Va sottoposta a gestione centrale controllata anche la tabella contenente i nomi dei Responsabili intestatari di delega all'autorizzazione delle richiesta d'acquisto, tabella utilizzata dalla procedura informatica che gestisce il ciclo autorizzativo. Analoga gestione controllata e centralizzata va adottata per la tabella contenente i nomi dei Responsabili che possono autorizzare l'emissione di un'Offerta/ Contratto di vendita. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- RS01P01 Procedura Gestione Acquisizione Contratti** **- RS02P01 Procedura Gestione Offerta Prima Qualificazione Fornitori** **- RS02P02 Procedura Gestione Fornitori** **- PGA11 Gestione Acquisto Vendita Partecipazioni Rami Azienda**

2.14 Delitti in materia di violazione del diritto d'autore (Art. 25-novies del D.Lgs. 231/01)

2.14.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-novies del Decreto richiama specificatamente i seguenti reati.

A) - Messa a disposizione del pubblico, in un sistema di reti telematiche,. di un'opera dell'ingegno protetta, o di parte di essa

B) - Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione o con usurpazione della paternità dell'opera...

C) - Abusiva duplicazione, per trarne profitto,... di programmi per elaboratore o, allo stesso scopo: importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale... di qualsiasi mezzo atto a rimuovere o a facilitare la rimozione... di dispositivi di protezione di un programma per elaboratore... o anche: ... riproduzione, trasferimento..., distribuzione, ... presentazione in pubblico..., vendita o concessione in locazione del contenuto di una banca dati

D) - Abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento,... di opere o parti di opera letterarie... ovvero multimediali... o banche dati...

E) - Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione

F) - Fraudolenta produzione, vendita,... installazione... di apparati... atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato...

La descrizione già fornita dei vari reati richiamati ci sembra sufficientemente esemplificativa delle varie fattispecie di reato.

2.14.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Direzioni commerciali
- Direzioni tecniche di produzione.

Si ritiene di non poter evidenziare **processi/sottoprocessi** più di altri **sensibili** rispetto al rischio di commissione dei reati qui considerati.

Modalità di commissione del reato.

Relativamente ai reati precedentemente elencati, di cui alle lettere E) ed F): il compimento di tali fattispecie di reato non sono neppure astrattamente ipotizzabili in Azienda.

Per quanto riguarda almeno una delle fattispecie di reato elencate dalla lettera A) alla D) comprese, si può astrattamente ipotizzare che in Azienda si verifichino una o entrambe le seguenti situazioni:

- si ha la disponibilità di un'opera dell'ingegno di Terzi quali, a titolo esemplificativo: un programma per elaboratore, una banca dati, una soluzione tecnologica, un documento o un'opera multimediale;

ovvero

- con riferimento ai diritti d'autore eventualmente connessi alle opere dell'ingegno sopra citate, si detengono mezzi intesi unicamente alla rimozione funzionale di dispositivi posti a protezione di tali diritti.

In tali circostanze, allo scopo di trarne profitto ed eventualmente previa rimozione dei dispositivi di protezione originariamente predisposti, l'Azienda potrebbe (con riferimento alle citate opere dell'ingegno):

- mettere a disposizione, su reti telematiche, un'opera dell'ingegno protetta (o parte di essa), con usurpazione della paternità dell'opera,

ovvero potrebbe

- abusivamente duplicare, riprodurre, trasferire, distribuire, diffondere in pubblico, vendere o dare in locazione un'opera dell'ingegno.

2.14.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.14.3.1 Principi generali di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2.

2.14.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
12 - 01	Sono espressamente vietati, in quanto lesivi del diritto d'autore, i seguenti comportamenti: - la ricezione, la diffusione o l'uso di software qualora tali operazioni risultino in contrasto con la dichiarata volontà del legittimo proprietario; - la detenzione o l'uso di software finalizzato a eludere o a forzare i sistemi di protezione dalla copia del software; - qualsiasi operazione finalizzata a compromettere l'integrità dei dati, la funzionalità o le prestazioni di sistemi informatici; - qualsiasi operazione finalizzata a eludere o forzare sistemi di controllo o sistemi informatici; - qualsiasi altro utilizzo vietato dalla legislazione vigente.	**- PGA02 Gestione Ciclo Passivo** **- RGP01 Regolamento uso risorse rete**

2.15 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies del D.Lgs. 231/01)

2.15.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-decies del Decreto richiama specificatamente il seguente reato: *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*.

Una semplice esemplificazione della fattispecie di reato è la seguente: con violenza, minaccia, offerta o promessa di denaro o altra utilità si induce una persona a non rendere dichiarazioni all'autorità giudiziaria o a rendere dichiarazioni mendaci.

2.15.2 Contestualizzazione aziendale e modalità di commissione

Rispetto al reato-presupposto qui richiamato, l'esposizione al rischio della Società è generale, nel senso che non si ritiene di poter segnalare **Soggetti/UU.OO**. particolarmente **sensibili**:

Lo stesso dicasi per l'individuazione dei **processi/sottoprocessi sensibili**.

Modalità di commissione del reato: nella previsione di procurare all'Azienda un illecito vantaggio, con minacce o promesse si induce una persona chiamata a rendere dichiarazioni davanti all'autorità giudiziaria a non renderle o a rendere dichiarazioni mendaci.

2.15.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.15.3.1 Principi specifici di comportamento

E' assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di questo reato.

Più in dettaglio è indispensabile:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- che si eviti qualsiasi comportamento che abbia lo scopo o l'effetto di indurre un soggetto terzo a rilasciare false dichiarazioni nell'ambito di un processo penale;
- che sia mantenuto un contegno chiaro, trasparente, diligente e collaborativo con le Pubbliche Autorità, con particolare riguardo alle Autorità Giudicanti ed Inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste.

2.16 Reati ambientali (Art. 25-undecies del D.Lgs. 231/01)

2.16.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25 *undecies* del Decreto, modificato dalla L. n. 68/15, richiama specificatamente i "Reati ambientali". Più precisamente, prevede una serie di sanzioni pecuniarie applicabili ad un Ente a fronte della commissione di una lunga serie di reati. Di seguito si riporta un elenco, *non esaustivo*, dei reati referenziati.

- Art. 452–bis del Codice Penale: inquinamento ambientale;
- art. 452–quater del Codice Penale: disastro ambientale;
- art. 452–quinquies del Codice Penale: disastro ambientale commesso con colpa;
- art. 452–octies del Codice Penale: associazione per delinquere e di stampo mafioso finalizzata a commettere uno qualsiasi dei delitti previsti nel nuovo Titolo VI–bis del Codice Penale;
- art. 452–sexies del Codice Penale: traffico e abbandono di materiale ad alta radioattività;
- Art. 452-quaterdecies del Codice Penale: Attività organizzate per il traffico illecito di rifiuti;
- art. 727-bis del Codice Penale: uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette;
- art. 733-bis del Codice Penale: distruzione o deterioramento di habitat all'interno di un sito protetto.

Con riferimento ai reati di cui all'art. 452–bis e 452–quater del Codice Penale, l'art. 25 – undecies del D.Lgs. 231/01 (così come modificato dalla Legge n. 68/2015) prevede che in caso di condanna si applichino all'ente, oltre alle sanzioni pecuniarie ivi previste, le sanzioni interdittive di cui all'art. 9 dello stesso D.Lgs. (per un periodo non superiore ad un anno nel caso di condanna per il delitto di cui all'art. 452–bis c.p.).

- Con riferimento al D.Lgs 152/06:
  - art. 137: scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili;

- art. 256: attività di gestione di rifiuti non autorizzata;
- art. 257: inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee;
- art. 258: violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari;
- art. 259: traffico illecito di rifiuti;
- art. 260-bis: false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti; nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti;
- art. 279, comma 5: emissioni nocive in atmosfera.

- Reati previsti o richiamati dagli artt. 1 commi 1 e 2, 2 commi 1 e 2, 3-bis comma 1 e 6 comma 4 della L. 150/92: importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie animali protette.
- Con riferimento alla L. n. 549/93, art. 3, comma 6: impiego di sostanze lesive dell'ozono stratosferico e dell'ambiente.
- Con riferimento al D.Lgs 202/07:
  - art. 8, commi 1 e 2: inquinamento doloso delle acque marine;
  - art. 9, commi 1 e 2: inquinamento colposo delle acque marine.

2.16.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai numerosi reato-presupposto qui richiamati, l'esposizione al rischio della Società appare circoscritto allo smaltimento dei rifiuti industriali costituiti da apparecchiature (o parti di apparecchiature) hardware giunte al termine del loro ciclo di vita o esaurite (es.: schermi video, apparecchiature fax, cartucce toner, ecc.).

Per quanto riguarda i **Soggetti/UU.OO**. particolarmente **sensibili**, la tipologia di reati considerati li individua:

- nella Dir. Acquisti e Affari Gen.li: addetti all'approvvigionamento di apparecchiature hardware di produzione e di consumo ed all'acquisizione di servizi di manutenzione;
- nel Responsabile del monitoraggio della corretta gestione dei rifiuti prodotti nelle varie sedi (c.d. "*Capo palazzo*").

Infine, per quanto concerne l'individuazione dei **processi/sottoprocessi sensibili**, per quanto appena affermato, si deve far riferimento ai processi di approvvigionamento del Ciclo Passivo, in particolare all'acquisizione di servizi di manutenzione relativi ad apparati e ad infrastrutture.

Modalità di commissione del reato: allo scopo di evitare i costi correlati, la Società, nell'attività di smaltimento dei rifiuti, omette di rispettare puntualmente le norme di legge da applicare con riferimento alle varie fattispecie di reato qui considerate.

2.16.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.16.3.1 Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2.

2.16.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
13 – 01	In tutti i contratti relativi alla effettuazione di servizi di manutenzione a seguito dei quali è prevedibile la produzione di rifiuti (materiale edile, materiale elettrico, scarti per manutenzione apparecchiature quali toner, etc.) è necessario che nel contratto con il fornitore sia espressamente richiesto che la rimozione di detto materiale è a carico del fornitore medesimo e che la stessa avvenga al termine di ciascuna giornata lavorativa.	**- PGA02 Gestione Ciclo Passivo** **- LGP15 Linee Guida per Smaltimento rifiuti**
13 – 02	Per quanto riguarda le norme da rispettare per la gestione delle cartucce (toner) delle stampanti, si rimanda a quanto precisato nella Linea Guida di riferimento.	**- LGP15 Linee Guida per Smaltimento rifiuti**
13 - 03	Per quanto riguarda le norme da rispettare per la dismissione/ rottamazione delle apparecchiature elettriche ed elettroniche, si rimanda a quanto precisato nella Linea Guida di riferimento.	**- LGA01 Linee Guida per dismissione cespiti**

2.17 Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies del D.Lgs. 231/01)

2.17.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 25-duodecies del Decreto contestualizza nel seguente modo il reato (di cui all'art. 22, comma 12-bis del D. Lgs. n. 286/1998) qui considerato:

un Datore di lavoro occupa alle proprie dipendenze lavoratori stranieri (extraeuropei)

- privi del permesso di soggiorno
- il cui permesso è scaduto e del quale non sia stato chiesto il rinnovo nei termini di legge
- il cui permesso è revocato o annullato

ed, in qualunque dei tre casi citati, si verifica una delle seguenti situazioni:

- i lavoratori occupati sono in numero superiore a tre;
- i lavoratori occupati sono minori in età non lavorativa;
- i lavoratori occupati sono sottoposti a condizioni di particolare sfruttamento di cui al 3° comma dell'art. 603-bis del codice penale (violazioni della normativa in materia di sicurezza e igiene nei luoghi di lavoro, tale da esporre il lavoratore a pericolo per la salute, la sicurezza o l'incolumità personale).

A seguito della modifica intervenuta con L. 17 ottobre 2017, n. 161, la responsabilità da reato dell'ente si estende anche ai reati di cui all'art. 12, commi 3, 3-bis, 3-ter e 5 del sopra citato D. Lgs. n. 286/1998 che puniscono:

- le attività di promozione, direzione, organizzazione, finanziamento, trasporto di stranieri nel territorio dello Stato ovvero qualsiasi altro atto diretto a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente nel caso in cui:

- a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;

b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumita' per procurarne l'ingresso o la permanenza illegale;

c) la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;

d) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;

e) gli autori del fatto hanno la disponibilità di armi o materie esplodenti (art. 12, comma 3)[4].

- la condotta di chi, al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero o nell'ambito delle attività punite a norma del presente articolo, favorisce la permanenza di questi nel territorio dello Stato in violazione delle norme del D. Lgs. n. 286/1998 (art. 5 D. Lgs. n. 286/1998).

2.17.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Dir. Gen. Human Resource & Organization
- Dir. Gen. Amm. Fin. e Controllo (Dir. Acquisti Consulenze Informatiche)

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Selezione ed assunzione di personale (subordinato o para-subordinato)
- Acquisizione di una prestazione di lavoro autonomo
- Gestione, nel tempo, del rapporto di collaborazione con un Dipendente o con un Lavoratore autonomo.

Modalità di commissione del reato: allo scopo di conseguire un vantaggio economico (quale potrebbe essere, ad esempio, il riconoscimento di un compenso inferiore a quello di mercato, a parità di competenze), la Società impiega personale extracomunitario non in regola con le norme previste per il soggiorno sul territorio nazionale.

2.17.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

[4] Ai sensi dell'art. 3-bis del D. Lgs. n. 286/1998 "*se i fatti di cui al comma 3 sono commessi ricorrendo due o più delle ipotesi di cui alle lettere a), b), c), d) ed e) del medesimo comma, la pena ivi prevista è aumentata*". Ai sensi del comma 3-ter del medesimo D. Lgs. n. 286/1998 "*la pena detentiva è aumentata da un terzo alla metà e si applica la multa di 25.000 euro per ogni persona se i fatti di cui ai commi 1 e 3: a) sono commessi al fine di reclutare persone da destinare alla prostituzione o comunque allo sfruttamento sessuale o lavorativo ovvero riguardano l'ingresso di minori da impiegare in attivita' illecite al fine di favorirne lo sfruttamento; b) sono commessi al fine di trame profitto, anche indiretto*".

2.17.3.1 Principi specifici di comportamento

- Nell'ambito del processo di acquisizione di una prestazione da parte di un Lavoratore autonomo, qualora si tratti di una persona extracomunitaria, è obbligatorio acquisire, prima del perfezionamento del rapporto contrattuale di collaborazione, copia del regolare e valido Permesso di soggiorno rilasciato al Lavoratore dalle Autorità competenti. Sempre prima del perfezionamento del rapporto contrattuale di collaborazione, è obbligatorio acquisire dal Lavoratore una sua dichiarazione sottoscritta con la quale egli si impegna: - a comunicare tempestivamente alla Società qualsiasi variazione di stato del Permesso di soggiorno (scadenza, rinnovo, sospensione o revoca); - in caso di rinnovo, a trasmettere copia del nuovo Permesso a lui rilasciato.

2.17.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
14 - 01	Nell'ambito del processo di selezione/assunzione di personale, sia che si tratti di un candidato ad una posizione di "stage", sia che si tratti di una persona candidata all'instaurazione di un rapporto di lavoro subordinato o para-subordinato, qualora si tratti di un Candidato extracomunitario, è obbligatorio acquisire, prima del perfezionamento del rapporto contrattuale di collaborazione, copia del regolare e valido *Permesso di soggiorno* rilasciato al Candidato dalle Autorità competenti. Sempre prima del perfezionamento del rapporto contrattuale di collaborazione, è obbligatorio acquisire dal Candidato una sua dichiarazione sottoscritta con la quale egli si impegna: - a comunicare tempestivamente alla Società qualsiasi variazione di stato del *Permesso di soggiorno* (scadenza, rinnovo, sospensione o revoca); - in caso di rinnovo, a trasmettere copia del nuovo *Permesso* a lui rilasciato. Per tutta la durata del contratto, la Direzione Amministrativa del Personale verifica il perdurare della validità del permesso ed all'approssimarsi della data di scadenza dello stesso – nel caso in cui il rapporto contrattuale fosse ancora in essere – avverte il Collaboratore della necessità di rinnovo.	**- PGP09 Gestione Risorse Umane**

2.18 Reati transnazionali – Induzione alla falsa testimonianza – Favoreggiamento personale (Art. 10 comma 9 della L. 146/06)

2.18.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui agli artt. 377-bis e 378 del Codice Penale, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per i seguenti reati "*transnazionali*":

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- Favoreggiamento personale

Per quanto riguarda il reato di "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*" si rimanda al medesimo reato precedentemente trattato con riferimento all'Art. 24-decies del D.Lgs 231/01.

Conviene precisare che l'art. 3 della citata Legge n. 146/06 definisce "*transnazionale*" un reato che veda coinvolto un gruppo criminale organizzato e che:

- sia commesso in più di uno Stato
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato
- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Esemplificazione della seconda fattispecie di reato qui considerata (con riferimento al contesto richiamato dal concetto di "reato transnazionale"): a seguito del compimento di un delitto per il quale la legge stabilisce la pena dell'ergastolo o la reclusione, si aiuta taluno a eludere le investigazioni dell'autorità, o a sottrarsi alle ricerche di questa.

2.18.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati non si rilevano **Soggetti/UU.OO. o processi particolarmente sensibili** da evidenziare.

La **modalità di commissione del reato** che si può astrattamente ipotizzare è la seguente.

In via del tutto generale, nelle relazioni personali verso Dipendenti o verso Terzi: adozione di comportamenti non rispettosi dei principi di legalità, correttezza e trasparenza.

2.18.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.18.3.1 Principi specifici di comportamento

Per quanto riguarda il reato di "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*" si rimanda al medesimo reato trattato con riferimento all'Art. 24-decies del D.Lgs 231/01.

E' comunque assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di uno dei reati qui considerati. Più in dettaglio è indispensabile:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- che sia mantenuto un contegno chiaro, trasparente, diligente e collaborativo con le Pubbliche Autorità, con particolare riguardo alle Autorità Giudicanti ed Inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste.

2.19 Reati transnazionali – Associazione per delinquere e di tipo mafioso (Art. 10 comma 2 della L. 146/06)

2.19.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui agli artt. 416 e 416-bis del Codice Penale, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per i seguenti reati "*transnazionali*":

- Associazione per delinquere
- Associazione di tipo mafioso

Relativamente al concetto di "*reato transnazionale*" si rimanda all'omologo precedente paragrafo relativo al primo dei *reati transnazionali* illustrati.

Con riferimento ai reati richiamati, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).

2.19.2 Contestualizzazione aziendale e modalità di commissione

Con riferimento ai reati richiamati, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).

2.19.3 Protocolli aziendali a presidio del rischio

Con riferimento ai reati richiamati, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).

2.20 Reati transnazionali – Associazione per delinquere, contrabbando di tabacchi (Art. 10 comma 2 della L. 146/06)

2.20.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui all'art. 291-quater del Decreto del Pres. della Rep. n. 43/73, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per il seguente reato "*transnazionale*":

- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri

Relativamente al concetto di "*reato transnazionale*" si rimanda all'omologo precedente paragrafo relativo al primo dei *reati transnazionali* illustrati.

Esemplificazioni delle fattispecie di reato qui considerate sono le seguenti.

Con riferimento al contesto richiamato dal concetto di "*reato transnazionale*" e, specificamente, al delitto di introduzione, vendita, trasporto, acquisto o detenzione nel territorio dello Stato di tabacco lavorato estero di contrabbando:

- tre o più persone si associano allo scopo di commettere più delitti
- un'associazione come quella di cui sopra viene promossa, costituita, diretta, organizzata o finanziata
- si è membri di un'associazione come quella di cui sopra.

2.20.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Vertice aziendale
- Dir. Gen. Amm. Fin. e Controllo
- Direzioni commerciali

I **processi/sottoprocessi sensibili** al rischio sono, in generale, i seguenti:

- Ciclo Passivo (acquisti ed approvvigionamenti)
- Ciclo Attivo (vendite).

La **modalità di commissione del reato** che si può astrattamente ipotizzare è la seguente.

In via del tutto generale: allacciamento e mantenimento di rapporti d'affari, economici o commerciali, di natura delittuosa con l'organizzazione di un Cliente, di un Fornitore o di un Partner.

2.20.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.20.3.1 Principi specifici di comportamento

E' assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di uno dei reati qui considerati. Più in dettaglio è indispensabile:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- che sia garantito il rispetto della normativa vigente, nonché delle procedure e dei protocolli aziendali, sia relativi al Ciclo attivo che a quello passivo, nonché quelli in materia di gestione ed impiego delle risorse e dei beni aziendali, in particolare per quelli di provenienza estera.

2.20.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
	.	
15 – 01	Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai *processi sensibili* rientranti nelle procedure di seguito elencate: → Gestione Anagrafica Fornitori: qualificazione e censimento nuovi Fornitori/modifica dati anagrafici e riferimenti bancari → Gestione Albo Fornitori qualificati: selezione Fornitori da Albo, valutazione Fornitori qualificati ed aggiornamento Albo → Gestione Ciclo passivo: autorizzazione alla spesa, analisi e sottoscrizione contratto, gestione fatturazione passiva e mandati di pagamento → Gestione Ciclo attivo: verifica e autorizzazione preventivi costi-ricavi, analisi e sottoscrizione contratto, gestione fatturazione attiva → Gestione Anagrafica Clienti: censimento nuovi Clienti/modifica dati anagrafici Deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Entrambi i tipi di contratto devono essere firmati da chi è dotato di apposita specifica Procura, così come documentato nel sistema di Procure gestito, sotto controllo, a livello centrale. Va sottoposta a gestione centrale controllata anche la tabella contenente i nomi dei Responsabili intestatari di delega all'autorizzazione delle richiesta d'acquisto, tabella utilizzata dalla procedura informatica che gestisce il ciclo autorizzativo. Analoga gestione controllata e centralizzata va adottata per la tabella contenente i nomi dei Responsabili che possono autorizzare l'emissione di un'Offerta/ Contratto di vendita. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- RS01P01 Procedura Gestione Acquisizione Contratti** **- RS02P01 Procedura Gestione Offerta Prima Qualificazione Fornitori** **- RS02P02 Procedura Gestione Fornitori**

2.21 Reati transnazionali – Associazione finalizzata al traffico di stupefacenti (Art. 10 comma 2 della L. 146/06)

2.21.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui all'art. 74 del Decreto del Pres. della Rep. n. 309/90, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per il seguente reato "*transnazionale*":

- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

Relativamente al concetto di "*reato transnazionale*" si rimanda all'omologo precedente paragrafo relativo al primo dei *reati transnazionali* illustrati.

Con riferimento al reato richiamato, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).

2.21.2 Contestualizzazione aziendale e modalità di commissione

Con riferimento al reato richiamato, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).

2.21.3 Protocolli aziendali a presidio del rischio

Con riferimento al reato richiamato, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).

2.22 Reati transnazionali – Immigrazioni clandestine (Art. 10 comma 7 della L. 146/06)

2.22.1 Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui all'art. 12 (commi: 3, 3-bis, 3-ter, 5) del D.Lgs. n. 286/98, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per il seguente reato "*transnazionale*":

- Immigrazioni clandestine

Relativamente al concetto di "*reato transnazionale*" si rimanda all'omologo precedente paragrafo relativo al primo dei *reati transnazionali* illustrati.

Esemplificazioni delle fattispecie di reato qui considerate sono le seguenti.

Con riferimento al contesto richiamato dal concetto di "*reato transnazionale*":

- al fine di trarre profitto anche indiretto, si compiono atti diretti a procurare l'ingresso di una persona nel territorio dello Stato in violazione delle disposizioni di legge, ovvero si procura l'ingresso illegale in altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, eventualmente allo scopo di destinare la persona alla prostituzione o comunque allo sfruttamento sessuale, ...
- al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero, si favorisce la permanenza di questi nel territorio dello Stato in violazione delle norme di legge.

2.22.2 Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Vertice aziendale
- Dir. Gen. Amm. Fin. e Controllo
- Direzioni commerciali
- Dir. Gen. Human Resource & Organization

I **processi/sottoprocessi sensibili** al rischio sono, in generale, i seguenti:

- Ciclo Passivo (acquisti ed approvvigionamenti)
- Ciclo Attivo (vendite)
- Gestione del Personale (assunzioni).

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- Nei rapporti con singole persone: adozione di comportamenti non rispettosi dei principi di legalità, correttezza e trasparenza

- Allacciamento e mantenimento di rapporti d'affari, economici o commerciali, di natura delittuosa con l'organizzazione di un Cliente, di un Fornitore o di un Partner.

2.22.3 Protocolli aziendali a presidio del rischio

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.22.3.1 Principi specifici di comportamento

E' assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di uno dei reati qui considerati. Più in dettaglio è indispensabile:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- che sia garantito il rispetto della normativa vigente, nonché delle procedure e dei protocolli aziendali, sia relativi al Ciclo attivo che a quello passivo, nonché quelli in materia di gestione ed impiego delle risorse e dei beni aziendali, in particolare per quelli di provenienza estera;
- che sia garantito il rispetto della normativa vigente in materia di immigrazione e di lavoro, con particolare riferimento a ciò che attiene il profilo della costituzione del rapporto lavorativo.

2.22.3.2 Protocolli e controlli specifici relativi ai processi aziendali

Id. Protoc.	Comportamento aziendale prescritto, protocolli e controlli applicati	Nome del documento aziendale di riferimento
16- 01	Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai *processi sensibili* rientranti nelle procedure di seguito elencate: → Gestione Anagrafica Fornitori: qualificazione e censimento nuovi Fornitori/modifica dati anagrafici e riferimenti bancari → Gestione Albo Fornitori qualificati: selezione Fornitori da Albo, valutazione Fornitori qualificati ed aggiornamento Albo → Gestione Ciclo passivo: autorizzazione alla spesa, analisi e sottoscrizione contratto, gestione fatturazione passiva e mandati di pagamento → Gestione Ciclo attivo: verifica e autorizzazione preventivi costi-ricavi, analisi e sottoscrizione contratto, gestione fatturazione attiva → Gestione Anagrafica Clienti: censimento nuovi Clienti/modifica dati anagrafici → Gestione Risorse Umane/Assunzione di personale Deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Entrambi i tipi di contratto devono essere firmati da chi è dotato di apposita specifica Procura, così come documentato nel sistema di Procure gestito, sotto controllo, a livello centrale. Va sottoposta a gestione centrale controllata anche la tabella contenente i nomi dei Responsabili intestatari di delega all'autorizzazione delle richiesta d'acquisto, tabella utilizzata dalla procedura informatica che gestisce il ciclo autorizzativo. Analoga gestione controllata e centralizzata va adottata per la tabella contenente i nomi dei Responsabili che possono autorizzare l'emissione di un'Offerta/ Contratto di vendita. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**- PGA02 Gestione Ciclo Passivo** **- PGA03 Gestione Ciclo Attivo** **- RS01P01 Procedura Gestione Acquisizione Contratti** **- RS02P01 Procedura Gestione Offerta Prima Qualificazione Fornitori** **- RS02P02 Procedura Gestione Fornitori** **- PGP09 Gestione Risorse Umane**

2.23 Inosservanza delle sanzioni interdittive (art. 23 D.Lgs. 231/01)

2.23.1 Reati richiamati dal D.Lgs. 231/01

Ai sensi dell'art. 23 del Decreto "*Chiunque, nello svolgimento dell'attività dell'ente a cui è stata applicata una sanzione o una misura cautelare interdittiva trasgredisce agli obblighi o ai divieti inerenti a tali sanzioni o misure, è punito con la reclusione da sei mesi a tre anni. 2. Nel caso di cui al comma 1, nei confronti dell'ente nell'interesse o a vantaggio del quale il reato è stato commesso, si applica la sanzione amministrativa pecuniaria da duecento e seicento quote e la confisca del profitto, a norma dell'articolo 19*."
Ai sensi del terzo comma della norma in commento, se dal reato sopra descritto l'ente ha tratto un profitto rilevante, si applicano le sanzioni interdittive, anche diverse da quelle in precedenza irrogate.

2.23.2 Contestualizzazione aziendale

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Organo Dirigente
- Direzione Affari Legali e Societari
- Funzioni Aziendali che gestiscono le autorizzazioni, le licenze o le concessioni rilasciate alla Società
- Funzioni Aziendali che hanno contatti con la Pubblica Amministrazione
- Funzioni Aziendali che gestiscono agevolazioni, finanziamenti, contributi o sussidi riconosciuti alla Società
- Funzioni Aziendali che gestiscono la pubblicizzazione di beni o servizi.

2.23.3 Protocolli aziendali a presidio del rischio

Di seguito princìpi e norme di comportamento che la Società si impegna a rispettare al fine di evitare la commissione del reato nel contesto aziendale.

2.23.3.1 Principi specifici di comportamento

E' assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento del reato considerato. Più in dettaglio:

- è necessario che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- è necessario prevedere l'obbligo di comunicazione tempestiva (vale a dire nel più breve tempo possibile) delle sanzioni e/o delle misure cautelari interdittive applicate alla Società, alle Funzioni Aziendali responsabili delle attività rispetto alle quali le sanzioni e le misure sono state disposte, nonché ai soggetti coinvolti nei medesimi processi produttivi, affinché ne abbiamo immediata conoscenza e possano agire, quindi, nel rispetto delle prescrizioni imposte dalla Autorità Giudiziaria;
- è necessario che tutte le attività e le operazioni svolte nel contesto aziendale e/o per conto della Società siano improntate al rispetto e all'osservanza degli obblighi e dei divieti inerenti alla sanzione o alla misura cautelare interdittiva eventualmente irrogata nei confronti dell'ente.