HydroGEA S.p.a.

Piazzale Duca d'Aosta, 28

33170 - Pordenone

Mappatura aree a rischio

(art. 6, D. Lgs. n. 231/01)

Titolo	Mappatura aree a rischio		
Emesso da	HydroGEA S.P.A.		
Approvato da	CDA		
Revisione	1	Data revisione	11/12/2015
	2	Data revisione	31/05/2018
	3	Data revisione	07/07/2018
	4	Data revisione	14/03/2023

SOMMARIO

1 REATI PRESUPPOSTO RILEVANTI

All'esito dell'analisi della realtà operativa sono emerse, quali categorie di reati-presupposto che potenzialmente potrebbero impegnare la responsabilità della Società, le seguenti:

- 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)1,
- Delitti informatici e trattamento illecito dei dati (Art. 24 bis)2,
- Delitti contro l'industria e il commercio (Art. 25 bis-1),
- Delitti di criminalità organizzata (Art. 24 ter),
- Concussione, induzione indebita a dare o promettere utilità e corruzione (Art. 25)1,
- Reati societari (Art. 25 ter),
- Reati di omicidio colposo e lesioni colpose con violazione delle norme per la prevenzione degli infortuni sul lavoro (Art. 25 septies),
- Ricettazione, riciclaggio, autoriciclaggio (Art. 25 octies),
- Delitti in materia di violazione del diritto d'autore (Art. 25 novies)2,
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25 decies),
- Reati ambientali (Art. 25 undecies),
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25 duodecies)
- Reati tributari (Art. 25 quinquiesdecies)
- Reati di contrabbando (Art. 25 sexiesdecies).

Le categorie di reati-presupposto contemplate dal Decreto, che all'esito delle attività di risk assessment, della realtà operativa e dei processi che caratterizzano la Società, sono state ritenute applicabili, ma con ridotte possibilità di concreta commissione dei reati, sono:

- Falsità in strumenti e segni di riconoscimento (Art. 25 bis),
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (Art. 25 quater),

---

1 Trattati nel Capitolo intitolato "Delitti contro la Pubblica Amministrazione". La frode informatica ai danni dello Stato o di altro Ente pubblico, pur annoverata fra i reati contro la PA, è analizzata nel Capitolo sui "Reati informatici" in quanto i protocolli di prevenzione del reato sono assimilabili a quelli per la prevenzione di tali reati.

2 Trattati nel Capitolo intitolato "Reati informatici".

- Delitti contro la personalità individuale (Art. 25 quinquies)
- Reati di contrabbando (Art. 25 sexiesdecies).

Le categorie di reati-presupposto contemplate dal Decreto, che all'esito delle attività di risk assessment, della realtà operativa e dei processi che caratterizzano la Società, sono state ritenute non applicabili sono:

- Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1),
- Abusi di mercato (Art. 25-sexies),
- Razzismo e xenofobia (Art. 25 terdecies).
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies).

Per ciascuna delle categorie di reati-presupposto considerate rilevanti per la Società sono state individuate nei paragrafi seguenti le attività a rischio nello svolgimento delle quali è astrattamente possibile che sia commesso uno dei reati nel seguito elencati e descritti.

1.1 Principi generali di comportamento

a) È vietato porre in essere comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, fattispecie di reato rientranti tra quelle considerate dal Decreto.

b) È proibito porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate al punto a), possano potenzialmente diventarlo.

c) Tutte le attività della Società nelle aree a rischio e le operazioni a rischio si svolgono in conformità alle leggi vigenti e alle disposizioni del Codice Etico nonché seguendo procedure organizzative improntate al principio, ove possibile, della separazione dei ruoli.

d) Le singole fasi di dette procedure devono rispondere al requisito della tracciabilità così da risultare individuabili, verificabili e trasparenti.

e) Ogni violazione, deroga o scostamento dalle norme e dai protocolli del presente MOD deve essere segnalata all'ODV con le modalità indicate nel Capitolo "Organismo di Vigilanza".

f) All'ODV sono forniti tutti i dati, le informazioni e i report menzionati come flussi informativi verso l'ODV alla fine di ciascun paragrafo della Sezione "Protocolli di Prevenzione e Gestione" del presente MOD.

2 DELITTI CONTRO LA PUBBLICA AMMINISTRAZIONE

2.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Richiesta di provvedimenti amministrativi alla PA (permessi, concessioni, autorizzazioni, licenze, iscrizioni ad albi o registri, deroghe, disposizioni attuative, … rivolte a Enti Locali, Provincia, Regione, VVF, Camera di commercio, Agenzia delle Entrate, …).

   Vengono qui in considerazione i rapporti che la Società ha, ad esempio, con AUSIR – "Autorità unica per i servizi idrici e i rifiuti" nella Regione Friuli-Venezia Giulia, Comuni, Regione, Ministeri, ANAS, FS, Genio Civle, ENEL, VV.FF., Esercito, ….

2) Gestione di attività comunicative e adempimenti verso la PA (a titolo esemplificativo e non già esaustivo: Consiglio di Bacino, ARERA - Autorità di Regolazione per Energia, Reti e Ambiente, ULSS, …).

3) Verifiche e ispezioni da parte della Pubblica Amministrazione ovvero di incaricati di pubblico servizio (es. ULSS, NAS, Agenzia delle Entrate, Guardia di Finanza, VV.FF., ULSS, Spisal, Arpav, Direzione Provinciale del Lavoro, INAIL, Organismi notificati, …).

4) Partecipazione a procedimenti giudiziari, stragiudiziali e arbitrati, di natura civile, amministrativa, tributaria, giuslavorista e penale.

5) Predisposizione e presentazione della documentazione necessaria all'ottenimento di erogazioni, contributi, finanziamenti, sovvenzioni o agevolazioni da parte di enti pubblici e corretto impiego dei fondi eventualmente ottenuti a seguito di tali erogazioni, contributi, finanziamenti, sovvenzioni o agevolazioni.

Aree a Rischio strumentali alla consumazione del reato:

6) Attività necessarie a prevenire o dirimere una controversia con soggetti terzi: accordi transattivi.

7) Gestione di donazioni, regalie ed elargizioni di denaro o altre utilità e vantaggi.

8) Gestione della cassa e rimborsi spese al personale.

9) Gestione delle spese di rappresentanza.

10) Selezione e assunzione di personale.

11) Gestione del personale.

12) Gestione degli acquisti di beni, servizi, appalti, prestazioni professionali.

13) Gestione delle utenze.

14) Gestione delle reti e degli impianti.

15) Gestione di misure e controlli.

16) Gestione della tesoreria.

17) Gestione del sistema informativo.

18) Stipulazione di accordi e di contratti.

2.2 Reati potenziali

Art. 24 – Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche

i. Malversazione a danno dello Stato (art. 316 bis c.p.)
ii. Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.)
iii. Truffa (art. 640 c.p.)
iv. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.)
v. Frode informatica (art. 640 ter c.p.)

Art. 25 – Concussione, induzione indebita a dare o promettere utilità e corruzione

i. Concussione (art. 317 c.p.)
ii. Corruzione per l'esercizio della funzione (art. 318 c.p.)
iii. Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)
iv. Circostanze aggravanti (art. 319 bis c.p.)
v. Corruzione in atti giudiziari (art. 319 ter c.p.)
vi. Induzione indebita a dare o promettere utilità (art. 319 quater c.p.)
vii. Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
viii. Pene per il corruttore (art. 321 c.p.)
ix. Istigazione alla corruzione (art. 322 c.p.)
x. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.)
xi. Traffico di influenze illecite (art. 346 bis c.p.)

2.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

a) Il reato di truffa e di truffa aggravata in danno dello Stato o altro ente pubblico e di malversazione potrebbe astrattamente realizzarsi:

- quando, ad esempio, nella predisposizione di documenti o dati da trasmettere agli enti pubblici competenti in materia tributaria, previdenziale e/o assistenziale, si forniscano informazioni non veritiere o incomplete supportate da artifici e raggiri, al fine di ottenere un ingiusto profitto per la Società o il versamento di imposte/contributi inferiori a quelli realmente dovuti.
- nel caso in cui si pongano in essere artifici o raggiri, ad esempio, comunicando dati non veri o incompleti o predisponendo una documentazione falsa, per ottenere finanziamenti o contributi pubblici quali ad esempio sovvenzioni / erogazioni correlate al ricorso ad ammortizzatori sociali.
- nel caso in cui le richieste di finanziamento per la formazione del personale mediante fondi interprofessionali bilaterali (Fondimpresa, Fondirigenti, …), progetti quadro L. 236/93, finanziamenti regionali, Fondo Sociale Europeo (FSE), finanziamenti provinciali, Inail, …, siano il frutto di dichiarazioni o documentazione mendaci, ovvero anche se lecitamente acquisiti detti finanziamenti siano utilizzati per scopi diversi dalla formazione.

b) I reati di corruzione potrebbero astrattamente realizzarsi:

- attraverso l'elargizione di donazioni, regalie, omaggi, denaro o altre utilità e vantaggi a pubblici ufficiali o incaricati di pubblico servizio,
- mediante l'acquisto di beni o servizi a prezzi gonfiati ovvero l'acquisto di beni o servizi "fittizi" o non necessari per la creazione, in concorso con terzi, di provviste di denaro o altre utilità,
- dando seguito alle segnalazioni o richieste pervenute da pubblici ufficiali o incaricati di pubblico servizio di avvalersi o favorire specifici soggetti in qualità di fornitori ovvero di assumere, promuovere, gratificare o favorire nella scelta determinati soggetti,
- concedendo sponsorizzazioni fittizie a beneficio di soggetti legati a funzionari pubblici.

c) La fattispecie di traffico illecito di influenze potrebbe realizzarsi:

- laddove l'intermediario indebitamente si faccia dare o promettere, a sé o ad altri, dal soggetto privato, denaro o altre utilità come prezzo della propria attività di mediazione verso un pubblico ufficiale o un incaricato di pubblico servizio;
- laddove l'intermediario si faccia dare o promettere, a sé o ad altri, denaro o altra utilità, per remunerare il pubblico agente.

d) Il reato di corruzione in atti giudiziari potrebbe astrattamente realizzarsi nel caso in cui taluno offra o prometta a un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere o altro funzionario) denaro o altra utilità per compiere o aver compiuto, omettere o aver omesso, ritardare o aver ritardato atti del suo ufficio

ovvero per compiere o aver compiuto atti contrari ai suoi doveri di ufficio allo scopo precipuo di favorire o danneggiare una parte in un processo civile, penale o amministrativo ovvero al fine di ottenere la positiva definizione di un procedimento giudiziario.

2.4 Principi generali di comportamento

a) Qualsiasi rapporto con funzionari pubblici o esercenti un pubblico servizio è corretto, formale, documentabile e attento alle molteplici implicazioni che da esso possono derivare.

b) I rapporti con la PA sono tenuti solo e soltanto dai dipendenti, membri di organi societari, collaboratori e/o consulenti esterni autorizzati dalla Società sulla base di procedure, mansionari, deleghe e/o procure.

c) È proibito ogni e qualsiasi comportamento che possa pregiudicare l'imparzialità e il buon andamento della PA.

d) È vietato utilizzare, produrre o presentare documenti falsi e dichiarazioni non veritiere al fine di ottenere dalla PA permessi, concessioni, autorizzazioni, iscrizione ad albi o registri, erogazioni, contributi, finanziamenti e ogni altra utilità o vantaggio.

e) È altresì proibito devolvere e utilizzare contributi, sovvenzioni o finanziamenti concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea per scopi diversi da quelli per cui sono stati accordati.

f) È vietato offrire denaro, beni, o altre utilità a pubblici ufficiali, incaricati di pubblico servizio o loro parenti al fine di ottenere concessioni, licenze e autorizzazioni da parte della PA ovvero al fine di assicurarsi – dalla PA o da Autorità di controllo e di vigilanza – trattamenti di favore.

g) Omaggi e regalie corrisposti a titolo di rappresentanza e/o di cortesia sono ammessi purché rientranti nella prassi aziendale e di modico valore, e comunque tali da non compromettere l'integrità o la reputazione di una delle parti e da non essere interpretati, da un osservatore imparziale, come finalizzati ad acquisire vantaggi in modo improprio.

h) Le attività di promozione e sponsorizzazione, le elargizioni, donazioni e contribuzioni sono attuate nel rispetto dei criteri di trasparenza, verificabilità, congruità e correttezza al fine di evitare ogni comportamento che possa essere interpretato come non conforme alle norme di legge.

i) È vietato ricorrere a forme di contribuzione che, pur assumendo formalmente la veste di sponsorizzazioni, attività promozionali, incarichi professionali e/o consulenze si risolvono nella realtà dei fatti in regalie, omaggi o doni in favore di pubblici ufficiali, incaricati di pubblico servizio o loro parenti al fine di ottenerne vantaggi di qualsiasi natura e specie.

j) Il reclutamento e l'assunzione del personale avviene secondo criteri oggettivi di individuazione delle necessità aziendali e delle competenze professionali dei candidati.

k) Il conferimento d'incarichi a professionisti e/o consulenti esterni ha luogo sussistendo concrete ed effettive esigenze con processo condiviso da più funzioni aziendali.

l) Tutti i beni e servizi necessari al conseguimento dello scopo sociale sono acquistati in base alle esigenze, con processo condiviso da più funzioni aziendali.

2.5 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli di prevenzione e gestione indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Richiesta di provvedimenti amministrativi (permessi, concessioni, autorizzazioni, licenze, iscrizioni ad albi o registri, deroghe, disposizioni attuative, …). Gestione di comunicazioni e adempimenti verso la PA. Verifiche e ispezioni da parte della PA o di incaricati di pubblico servizio.	PT 01 – "Rapporti con la Pubblica Amministrazione"
Partecipazione a procedimenti giudiziari, stragiudiziali e arbitrati. Attività necessarie a prevenire o dirimere una controversia con soggetti terzi: accordi transattivi.	PT 02 – "Contenzioso"

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Predisposizione e presentazione della documentazione necessaria all'ottenimento di erogazioni, contributi, finanziamenti, sovvenzioni o agevolazioni da parte di enti pubblici e corretto impiego dei fondi eventualmente ottenuti.	PT 03 – "Finanziamenti pubblici"
Gestione di sponsorizzazioni, donazioni, regalie ed elargizioni di denaro o altre utilità e vantaggi.	PT 04 – "Sponsorizzazioni e donazioni"
Gestione delle operazioni per cassa. Gestione dei rimborsi spese al personale.	PT 05 – "Pagamenti per cassa e rimborsi spese al personale"
Gestione delle spese di rappresentanza.	PT 06 – "Spese di rappresentanza"
Selezione e assunzione di personale. Gestione amministrativa del personale.	PT 07 – "Selezione, assunzione e gestione del personale"
Gestione degli acquisti di beni, servizi e prestazioni professionali.	PT 08 – "Acquisti"
Gestione utente Gestione misure	PT 09 – "Gestione utenza"
Gestione reti ed impianti Gestione controlli	PT 10 – "Gestione reti e impianti"
Gestione della tesoreria, gestione dei pagamenti e degli incassi.	PT 09 – "Gestione utenza" PT 12 – "Risorse finanziarie"
Gestione del sistema informativo.	PT 15 – "Sistema informativo"
Emissione di ordini di acquisto, stipulazione di accordi e di contratti.	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione del presente MOD "Protocolli di prevenzione e di gestione".

3 REATI INFORMATICI

3.1 Attività a rischio

I cosiddetti "Reati Informatici" sono quei reati "commessi avvalendosi di un sistema informatico o in suo danno ovvero che pongano in qualsiasi modo l'esigenza di raccogliere prove in forma informatica". Essi trovano come presupposto l'impiego anomalo di strumenti e di tecnologie informatiche/telematiche, normalmente impiegati per lo svolgimento delle ordinarie attività professionali.

Nel novero degli illeciti commessi avvalendosi di sistemi informatici sono ricompresi:

A. Delitti informatici e trattamento illecito dei dati,

B. Frode informatica ai danni dello stato o di altri enti pubblici,

C. Delitti in materia di violazione del diritto d'autore, con riferimento alla detenzione e utilizzo di software di cui non si dispone della relativa licenza d'uso.

In considerazione della peculiarità dell'attività aziendale svolta, sono state individuate le seguenti Aree a Rischio Reato:

1) Gestione degli acquisti di beni, servizi, consulenze e prestazioni professionali.

2) Sviluppo, implementazione, utilizzo e manutenzione dell'infrastruttura tecnologica e del sistema informativo.

3) Protezione fisica dei dati, delle informazioni e dei sistemi.

4) Emissione di ordini di acquisto, stipulazione di accordi e di contratti.

3.2 Reati potenziali

<u>Art. 24 – 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</u>

i. Frode informatica (art. 640 ter c.p.).

<u>Art. 24 bis – Delitti informatici e trattamento illecito di dati</u>

ii. Documenti informatici (art. 491 bis c.p.),

iii. Accesso abusivo a un sistema informatico o telematico (art. 615 ter c.p.),

iv. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.),

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

vi. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.),

vii. Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.),

viii. Danneggiamento d'informazioni, dati e programmi informatici (art. 635 bis c.p.),

ix. Danneggiamento d'informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.),

x. Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.),

xi. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.),

Art. 25 novies – Delitti in materia di violazione del diritto d'autore

xii. Art. 171 Legge 22 aprile 1941, n. 633,

xiii. Art. 171 bis Legge 22 aprile 1941, n. 633,

xiv. Art. 171 ter Legge 22 aprile 1941, n. 633,

xv. Art. 171 septies Legge 22 aprile 1941, n. 633.

3.3 Esemplificazione delle modalità attraverso le quali potrebbe essere commesso il reato

a) Nella truffa o frode in danno dello Stato o di ente pubblico il reato potrebbe astrattamente realizzarsi qualora venisse modificato il sistema informatico di una PA al fine di inserire un importo relativo a un'imposta inferiore a quello dovuto legittimamente.

b) Tutti gli illeciti relativi alla falsità in atti pubblici disciplinati dal Codice Penale, tra i quali rientrano sia le falsità ideologiche[3] che le falsità materiali[4], sono punibili

[3] Si ha "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere.

[4] Si ha "falsità materiale" quando un documento non proviene dalla persona che risulta essere il mittente o da chi risulta dalla firma (contraffazione) ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.

anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico. I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali. A titolo esemplificativo, nell'alterazione di registri e documenti informatici, pubblici o privati, aventi efficacia probatoria, il delitto potrebbe astrattamente realizzarsi da chi falsifichi documenti aziendali oggetto di flussi informatizzati con una Pubblica Amministrazione o la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati "sensibili" in vista di una possibile attività ispettiva.

c) L'accesso abusivo al proprio sistema informativo o alla rete aziendale o al sistema informativo di soggetti pubblici o privati si realizza quando un soggetto s'introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza. A tal riguardo, si sottolinea come il legislatore abbia inteso punire l'accesso abusivo a un sistema informatico o telematico *tout court*, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente a un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi a eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura). La suddetta fattispecie delittuosa potrebbe astrattamente realizzarsi altresì nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato. Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto (hacker) acceda abusivamente ai sistemi informatici di proprietà di terzi, per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, o acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa.

d) Nella detenzione e utilizzo abusivo di codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informativo o alla rete aziendale o a un sistema informativo o alla rete di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate, l'illecito potrebbe astrattamente realizzarsi qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare

ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo. Pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. Tali fattispecie si configurano sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di accesso (ad esempio, un operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. Inoltre, è punito chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

e) L'acquisto di apparecchiature e/o software allo scopo di danneggiare un sistema informativo o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o a esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici. Tale delitto potrebbe astrattamente realizzarsi qualora un dipendente si procuri un virus idoneo a danneggiare o a interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione a un procedimento penale a carico della società.

f) Nello svolgimento di attività fraudolenta d'intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informativo o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate, il reato potrebbe astrattamente realizzarsi qualora un soggetto fraudolentemente intercetti comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione. Attraverso tecniche d'intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni

tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione. Il reato potrebbe astrattamente realizzarsi, ad esempio, con il vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione a una trattativa commerciale.

g) Nell'istallazione di apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati il reato potrebbe astrattamente realizzarsi quando qualcuno, al di fuori dai casi consentiti dalla legge, installi apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi. La condotta vietata è, pertanto, costituita dalla semplice installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva. Il reato potrebbe astrattamente realizzarsi, ad esempio, a vantaggio della società, nel caso in cui un dipendente s'introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione a una futura negoziazione.

h) La distruzione, danneggiamento, inservibilità d'informazioni, dati e programmi informatici e in particolare di quelli utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità; distruzione, danneggiamento, inservibilità di sistemi informatici o telematici e in particolare di sistemi informatici o telematici di pubblica utilità potrebbe astrattamente realizzarsi quando: i) un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. Il danneggiamento potrebbe essere commesso a vantaggio della Società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della Società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti"; ii) un soggetto commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Tale delitto si distingue dal precedente poiché, in

questo caso, il danneggiamento ha per oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica. Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi a un procedimento penale a carico della società; iii) quando un soggetto attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Pertanto, qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati. Questo reato potrebbe astrattamente realizzarsi quando la condotta di cui al precedente punto sia diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o a ostacolarne gravemente il funzionamento. Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità, quel che si rileva in primo luogo è che il danneggiamento deve avere per oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

i) Nei delitti in materia di violazione del diritto d'autore il reato potrebbe astrattamente realizzarsi laddove si proceda all'installazione, duplicazione, detenzione e utilizzo di software di proprietà di terzi sulle macchine aziendali (client, server, apparati di rete, telefoni, tablet, …) per i quali non si disponga della relativa licenza o la stessa sia scaduta.

3.4 Principi generali di comportamento

Gli organi sociali della Società, i dipendenti e i consulenti della stessa hanno l'obbligo di:

a) rispettare le norme di legge, il Codice Etico e il presente MOD, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino i reati informatici come sopra delineati;

b) rispettare le norme, le procedure, le istruzioni, i regolamenti e le disposizioni operative od organizzative che disciplinano l'accesso e l'utilizzo dei sistemi e degli

applicativi informatici della Società;

c) porre in essere tutte le attività di gestione delle risorse informatiche correttamente e legalmente, in modo trasparente e collaborativo utilizzando le medesime risorse con la massima attenzione e professionalità evitando comportamenti che, benché risultino tali da non costituire di per sé specifici "Reati informatici", lo possano potenzialmente diventare;

d) evitare qualsiasi situazione di conflitto di interessi nei confronti di terzi esterni in relazione a quanto previsto dalle ipotesi di reato informatico.

e) rispettare la normativa nazionale e comunitaria sulla privacy.

3.5 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione degli acquisti di beni, servizi, consulenze e prestazioni professionali	PT 08 – "Acquisti"
Sviluppo, implementazione, utilizzo e manutenzione dell'infrastruttura tecnologica. Gestione del sistema informativo aziendale. Protezione fisica dei dati, delle informazioni e dei sistemi	PT 15 – "Sistema informativo"
Emissione di ordini di acquisto, stipulazione di accordi e di contratti	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

4 DELITTI DI CRIMINALITÀ ORGANIZZATA

4.1 Attività a rischio

In considerazione della particolare natura dei delitti di criminalità organizzata nazionale e transnazionale, tutte le aree aziendali considerate a rischio per i reati presupposto di responsabilità ai sensi del Decreto contemplate nel presente Modello sono potenzialmente a rischio anche per i reati associativi; infatti, essi rappresentano una mera modalità, l'associazione per l'appunto, di commissione dei reati c.d. "fine"; pertanto, tali reati propagano la presenza del rischio a tutte le aree mappate e sono da considerare a rischio diffuso.

4.2 Reati potenziali

i. Associazione per delinquere (art. 416 c.p.),

ii. Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.)

4.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

Il reato potrebbe astrattamente realizzarsi qualora:

a) esponenti della Società, il fiscalista di riferimento e un soggetto terzo, utilizzino fatture o altri documenti di quest'ultimo emessi per operazioni inesistenti, nella formazione delle dichiarazioni dei redditi;

b) un soggetto apicale della Società agevoli l'attività di un'associazione di tipo mafioso, stipulando contratti di fornitura con fornitori affiliati alla predetta associazione, o comunque indicati da esponenti affiliati alla predetta associazione, ottenendone in cambio vantaggi diretti o indiretti grazie all'influenza esercitata sul territorio dall'associazione di tipo mafioso;

c) un esponente della Società agevoli l'attività di un'associazione di tipo mafioso, concludendo un contratto di consulenza con un soggetto affiliato a detta associazione senza verificarne i requisiti di onorabilità, al fine di agevolare detta associazione;

d) un soggetto apicale concluda un contratto per sponsorizzare un ente, ovvero elargisca liberalità a un ente svolgente attività apparentemente lecita, ma in realtà affiliato a un'associazione di tipo mafioso, al fine di agevolarne l'attività e sfruttare la forza intimidatrice dell'associazione mafiosa per ottenere vantaggi;

e) un soggetto sottoposto e/o soggetto apicale si accordi con due o più soggetti, anche estranei alla Società al fine di eseguire illecitamente la miscelazione e lo smaltimento di rifiuti tramite la simulazione di operazioni di selezione, trattamento e recupero, falsificazione di documenti analitici e di trasporto;

f) un esponente della Società paghi un affiliato a un'organizzazione criminale per poter recuperare i dati aziendali crittografati e resi inservibili da un software malvagio introdotto fraudolentemente nel proprio sistema informatico.

4.4 Principi generali di comportamento

Gli organi sociali della Società, i dipendenti e i consulenti della stessa hanno l'obbligo di:

a) rispettare le norme di legge, il Codice Etico e il presente MOD, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino i delitti di criminalità informatica come sopra delineati;

b) astenersi dall'intraprendere rapporti o iniziative nei confronti di enti pubblici o privati di cui sia nota o sospettata l'infiltrazione da parte di soggetti appartenenti a organizzazioni criminali.

4.5 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio, la Società ha adottato l'insieme dei protocolli riportati nella successiva Sezione "Protocolli di prevenzione e di gestione" del presente Modello.

5 DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

5.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Gestione degli utenti e del processo di vendita dei servizi;

2) Gestione delle reti e degli impianti;

3) Gestione degli acquisti di beni, servizi, consulenze e prestazioni professionali.

5.2 Reati potenziali

i. Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.).

5.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

Il reato potrebbe astrattamente realizzarsi:

a) laddove la Società fornisse acqua potabile agli utenti senza rispettare le caratteristiche quantitative / qualitative contrattualmente definite con gli utenti e con le competenti autorità (ad esempio una pressione di pompaggio nella rete di distribuzione inferiore ai valori richiesti);

b) laddove la Società fornisse agli utenti acqua potabile senza rispettare i parametri qualitativi prescritti dalle normative sanitarie, ad esempio risparmiando sul contenuto di cloro per la potabilizzazione;

c) se la Società dovesse fatturare una quantità di acqua superiore a quella effettivamente consumata dagli utenti per effetto di letture non corrette del contatore, errori di misura del contatore, fatturazioni in eccesso rispetto alle letture rilevate, fatturazione di consumi con corrispondenti tariffe non consone

5.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione degli acquisti di beni, servizi, consulenze e prestazioni professionali.	PT 08 - "Acquisti"
Gestione reti ed impianti Gestione controlli	PT 10- "Gestione reti e impianti"
Gestione della tesoreria, gestione dei pagamenti e degli incassi.	PT 09 – "Gestione utenza" PT 12 – "Risorse finanziarie"
Emissione di ordini di acquisto, stipulazione di accordi e di contratti.	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

6 REATI SOCIETARI

6.1 Attività a rischio

In considerazione della peculiarità dell'attività aziendale svolta, sono state individuate le seguenti Aree a Rischio Reato:

1) Redazione e tenuta delle evidenze economico–patrimoniali relative all'attività/produzione economica tipica.
2) Redazione e tenuta delle scritture contabili.
3) Elaborazione, valutazione e illustrazione dei dati e delle informazioni necessarie alla predisposizione del bilancio e delle altre comunicazioni sociali previste dalla legge e, più in generale, di qualunque documento giuridicamente rilevante nel quale si evidenzino elementi economici, patrimoniali e finanziari dell'impresa.
4) Predisposizione delle dichiarazioni fiscali e liquidazione dei relativi importi.
5) Accesso, gestione e aggiornamento del piano dei conti e delle registrazioni contabili tramite il sistema gestionale aziendale.
6) Gestione dei rapporti con i Soci.
7) Operazioni relative al capitale sociale.
8) Gestione degli adempimenti societari.

Aree a Rischio strumentali alla consumazione del reato:

9) Gestione dell'utenza, dei servizi erogati e dei crediti
10) Gestione del sistema informativo aziendale.
11) Gestione dei rapporti con gli istituti di credito e gli intermediari finanziari.
12) Gestione della tesoreria.

6.2 Reati potenziali

i. False comunicazioni sociali (art. 2621 c.c.).

ii. Fatti di lieve entità (art. 2621 bis c.c.).

iii. Impedito controllo (art. 2625 c.c.).

iv. Indebita restituzione dei conferimenti (art. 2626 c.c.).

v. Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.).

vi. Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.).

vii. Operazioni in pregiudizio dei creditori (art. 2629 c.c.).

viii. Formazione fittizia del capitale (art. 2632 c.c.).

ix. Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.).

x. Corruzione tra privati (art. 2635 c.c.)[5].

xi. Istigazione alla corruzione tra privati (art. 2635 bis c.c.)[6]

xii. Illecita influenza sull'assemblea (art. 2636 c.c.).

xiii. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

6.3 Esemplificazione delle modalità attraverso le quali potrebbe essere commesso il reato

Il reato potrebbe astrattamente realizzarsi:

a) ad opera di amministratori, direttori, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, liquidatori e consulenti i quali, 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 previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, ovvero omettono informazioni, la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della Società, in modo idoneo a indurre in errore i destinatari sulla predetta situazione.

b) Mediante inserimento nel Sistema Informativo Aziendale di dati contabili alterati o invalidi.

---

5 Ai fini dell'applicabilità del Decreto rilevano i casi previsti dal terzo comma del presente articolo

6 Ai fini dell'applicabilità del Decreto rilevano i casi previsti dal primo comma del presente articolo.

c) laddove la Società fatturasse consumi di acqua superiori a quelli effettivamente realizzati fornendo dati ed informazioni sullo stato economico e patrimoniale falsi rispetto alla reale situazione societaria.

d) Allorquando gli amministratori impediscano od ostacolino, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo attribuite ai soci o ad altri organi sociali.

e) Attraverso la restituzione, anche simulata, da parte degli Amministratori stessi dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli ovvero nella ripartizione da parte degli Amministratori di utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite ovvero con l'acquisto o la sottoscrizione da parte degli Amministratori, di azioni o quote sociali riferite alla Società o a una società controllata, da cui derivi una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, ovvero con l'effettuazione da parte degli Amministratori, e in violazione delle disposizione di legge a tutela dei creditori, di operazioni di riduzione del capitale sociale o fusioni con altre società o scissioni che cagionino danno ai creditori.

f) Quando viene formato o aumentato fittiziamente il capitale della Società mediante le condotte descritte esaustivamente dal legislatore.

g) Quando un Amministratore presenti all'Assemblea, in relazione a un determinato ordine del giorno, atti e documenti falsi o non completi o comunque alterati nei contenuti, allo scopo di indurre l'Assemblea ad approvare una puntuale delibera su uno specifico argomento.

h) Attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero ancorché oggetto di valutazione, sulla situazione economico patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

6.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione della logistica in entrata e dei magazzini.	PT 08 – "Acquisti"
Gestione reti ed impianti Gestione controlli	PT 10 – "Gestione reti e impianti"
Gestione della tesoreria, gestione dei pagamenti e degli incassi.	PT 09 – "Gestione utenza" PT 12 – "Risorse finanziarie"
Redazione e tenuta delle evidenze economico-patrimoniali relative all'attività / produzione economica tipica. Redazione e tenuta delle scritture contabili. Accesso, gestione e aggiornamento del piano dei conti e delle registrazioni contabili tramite il sistema gestionale aziendale. Elaborazione, valutazione e illustrazione dei dati e delle informazioni necessarie alla predisposizione del bilancio e delle altre comunicazioni sociali. Predisposizione delle dichiarazioni fiscali e liquidazione dei relativi importi.	PT 11 – "Bilancio e dichiarazioni fiscali"
Gestione dei rapporti con i Soci.	PT 13 – "Rapporti con i Soci"
Gestione delle operazioni relative al capitale sociale. Gestione degli adempimenti societari.	PT 14 – "Operazioni relative al capitale sociale e adempimenti societari"
Gestione del sistema informativo aziendale	PT 15 – "Sistema informativo"

Per prendere visione dei protocolli sopra richiamati si rinvia al successivo capitolo "Protocolli di prevenzione e di gestione".

7 DELITTI CONTRO LA PERSONALITA' INDIVIDUALE

7.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Selezione, assunzione e gestione di personale.
2) Gestione e controllo dei rimborsi spese al personale.
3) Sviluppo, implementazione, utilizzo e manutenzione dell'infrastruttura tecnologica e del sistema informativo.
4) Protezione fisica dei dati e dei sistemi.
5) Emissione di ordini di acquisto, stipulazione di accordi e di contratti.

7.2 Reati potenziali

i. Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.),
ii. Pornografia virtuale (art. 600 quater.1 c.p.),
iii. Tratta di persone (art. 601 c.p.),
iv. Intermediazione illecita di manodopera (art. 603 bis c.p.)

7.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

Il delitto potrebbe astrattamente realizzarsi:

a) affidando la produzione dei propri prodotti e l'erogazione dei propri servizi a società terze (fornitori, terzisti, trasportatori, appaltatori, subappaltatori), aventi sede in Italia o all'estero, le quali costringono i propri dipendenti a turni di lavoro che ne comportano, di fatto, la riduzione in schiavitù.
b) Distribuendo, divulgando, diffondendo e detenendo materiale pornografico e/o pedopornografico attraverso i sistemi informatici della Società.
c) Mediante abuso di autorità, inganno, abuso di stato di sudditanza psicologica o stato di necessità, promessa e/o dazione di danaro o altri benefici, costringendo un dipendente o un collaboratore a prestazione lavorative, sessuali o di altra

natura che ne comportino lo sfruttamento o ne ledano la libertà, incolumità e dignità.

d) Mediante il reclutamento di manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori.

e) Utilizzando, assumendo o impiegando – anche mediante l'attività di intermediazione – lavoratori sottoposti a condizioni di sfruttamento e approfittando dello stato di bisogno degli stessi lavoratori.

7.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione delle operazioni per cassa Gestione dei rimborsi spese al personale.	PT 05 – "Pagamenti per cassa e rimborsi spese al personale"
Selezione e assunzione del personale. Gestione amministrativa del personale.	PT 07 – "Selezione, assunzione e gestione del personale"
Gestione del sistema informativo aziendale. Protezione fisica dei dati e dei sistemi.	PT 15 – "Sistema informativo"
Emissione di ordini di acquisto, stipulazione di accordi e di contratti.	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

8 REATI DI OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE CON VIOLAZIONE DELLE NORME PER LA PREVENZIONE DEGLI INFORTUNI SUL LAVORO

8.1 Attività a rischio

In riferimento ai reati relativi alla violazione delle norme per la prevenzione degli infortuni, le Linee Guida di Confindustria evidenziano che, aprioristicamente, non è possibile escludere dall'inventariazione delle aree a rischio alcun ambito di attività poiché tali reati potrebbero interessare la totalità delle componenti aziendali.

Per quanto attiene l'individuazione e l'analisi dei rischi potenziali, le Linee Guida rilevano che l'analisi delle possibili modalità attuative coincide con la valutazione dei rischi lavorativi effettuata dalla Società sulla scorta della legislazione prevenzionistica vigente.

I rischi lavorativi presenti negli ambienti di lavoro possono essere divisi in tre grandi categorie:

- Rischi per la sicurezza;
- Rischi per la salute;
- Rischi per la sicurezza e la salute o rischi di tipo trasversale.

Rischi per la sicurezza

I rischi per la sicurezza o rischi di natura infortunistica sono quelli collegabili al potenziale verificarsi degli incidenti e/o degli infortuni in particolare presso luoghi di lavoro esterni alle aree di pertinenza aziendale (ad esempio presso cantieri esterni oggetto di appalto).

Le cause di tali rischi sono da ricercare in un assetto non idoneo delle caratteristiche di sicurezza proprie dell'ambiente di lavoro, nelle macchine e/o apparecchiature utilizzate, nelle modalità operative, nell'organizzazione del lavoro, ecc..

I rischi per la sicurezza di cui ci occupiamo possono quindi essere suddivisi nei seguenti gruppi:

- Rischi derivanti da carenze strutturali dell'ambiente di lavoro;
- Rischi derivanti da carenza di protezione su macchine e apparecchiature;
- Rischi derivanti da insufficiente protezione elettrica;

- Rischi derivanti da situazioni di emergenza quali incendio o esplosione.

Rischi per la salute

I rischi per la salute o rischi igienico-ambientali sono quelli responsabili della potenziale compromissione dell'equilibrio biologico del personale addetto a operazioni o a lavorazioni che comportano l'emissione nell'ambiente di "fattori ambientali di rischio" di natura chimica, fisica, biologica.

I rischi per la salute possono essere quindi raggruppati in:

- Rischi derivanti da agenti chimici;
- Rischi derivanti da agenti fisici.

Rischi per la sicurezza e la salute

I rischi per la sicurezza e la salute (rischi trasversali) sono individuabili all'interno del rapporto tra il lavoratore e l'organizzazione del lavoro in cui lo stesso è inserito. Tale rapporto è a sua volta immerso in un quadro di compatibilità e interazioni che sono contemporaneamente di tipo ergonomico, psicologico e organizzativo.

I rischi per la sicurezza e la salute sono essenzialmente dovuti a:

- organizzazione del lavoro;
- fattori psicologici;
- fattori ergonomici.

In considerazione della peculiarità dell'attività svolta, sono state individuate le seguenti aree a Rischio:

1) Erogazione ed efficacia di azioni di informazione, addestramento e formazione dei lavoratori con particolare riferimento alle lavorazioni svolte presso luoghi di lavoro esterni alle sedi aziendali
2) Monitoraggio dell'applicazione continua e sistematica delle misure di prevenzione e protezione (definizione dei soggetti responsabili, definizione dei parametri di riferimento; segnalazioni di non conformità, comportamenti pericolosi, mancati infortuni)
3) Applicazione ed efficacia delle misure di prevenzione e protezione per tutte le attrezzature (macchine, impianti, utensili, etc.) utilizzate per la realizzazione dei processi operativi aziendali, comprendenti le infrastrutture in uso in tutte le aree operative interne ed esterne all'azienda (sedi di appalto)

4) Struttura del sistema aziendale per la gestione della sicurezza (politica, pianificazione degli obiettivi, assetto organizzativo con definizione dei ruoli e delle responsabilità)
5) Nomina delle figure previste dalla normativa vigente (Responsabile del Servizio di Prevenzione e Protezione, Medico Competente, Rappresentante dei Lavoratori per la Sicurezza);
6) Riesame periodico del sistema di gestione della sicurezza (contenuti della Riunione periodica, momenti di verifica sul mantenimento nel tempo dell'efficacia delle procedure interne)
7) Gestione della normativa cogente (capacità di reazione al cambiamento normativo e alle scadenze previste) e gestione della documentazione (accessibilità dei documenti e reperibilità)
8) Effettuazione della valutazione dei rischi relativo aggiornamento (elaborazione del documento di valutazione), compresi i rischi derivanti dalle interferenze nel caso di processi oggetto di appalto;
9) Applicazione ed efficacia delle misure di prevenzione dei rischi derivanti da emergenza sanitaria (primo soccorso), incendio ed emergenza in genere;
10) Organizzazione della gestione delle emergenze
11) Gestione delle sostanze pericolose
12) Gestione della sorveglianza sanitaria

8.2 Reati potenziali

i. Omicidio colposo (art. 589 c.p.)
ii. Lesioni colpose gravi o gravissime (art. 590 c.p.)

8.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

Per lesioni gravi s'intendono quelle che determinano:

- una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai 40 giorni;
- l'indebolimento permanente di un senso o di un organo.

Per lesioni gravissime s'intendono quelle che determinano:

- una malattia certamente o probabilmente insanabile;
- la perdita di un senso;
- la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità;
- la deformazione, ovvero lo sfregio permanente del viso.

I reati colposi in oggetto acquistano rilevanza dal punto di vista della responsabilità amministrativa della persona giuridica qualora siano conseguenza di violazioni della normativa di riferimento in materia di tutela dell'igiene e della salute sul lavoro e, in particolare, in via puramente esemplificativa ma non esaustiva, nelle seguenti ipotesi:

a) mancata o inadeguata effettuazione della valutazione dei rischi, anche in relazione ai rischi di interferenza e relativi a sedi esterne;

b) mancata o inadeguata elaborazione dei relativi documenti e del loro periodico aggiornamento (DVR e DUVRI);

c) omissione di predisposizione ovvero rimozione o danneggiamento di impianti, apparecchi e/o strumenti di segnalazione destinati alla prevenzione di disastri e/o infortuni sul lavoro (omissione o rimozione delle cautele antinfortunistiche) e/o di dispositivi di protezione

d) uso scorretto di attrezzature di lavoro, sostanze e preparati pericolosi, mezzi di trasporto

e) mancata vigilanza sul comportamento dei lavoratori

f) mancata o inadeguata messa a disposizione di idonei dispositivi di protezione collettiva e/o individuale;

g) omissione nella collocazione ovvero rimozione o danneggiamento tale da renderli inservibili all'uso di apparecchi o altri strumenti destinati alla estinzione di un incendio ovvero al salvataggio o soccorso in caso di disastro o infortunio sul lavoro;

h) mancata erogazione della formazione / informazione / addestramento ai lavoratori prevista dalla normativa vigente;

i) mancata designazione del Medico Competente alla sorveglianza sanitaria delle condizioni di lavoro e dei lavoratori ovvero designazione di un soggetto non in possesso di adeguata esperienza, formazione e preparazione professionale;

j) mancata designazione del Responsabile Servizio Prevenzione e Protezione (RSPP) ovvero designazione di un soggetto non in possesso di adeguata esperienza, formazione e preparazione professionale.

8.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Tutti i processi che coinvolgono o che influenzano i lavoratori esponendoli al rischio di infortunio o malattia professionale	PT 16 - "Salute e sicurezza sui luoghi di lavoro"
Emissione di ordini, stipulazione di accordi, contratti	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

9 RICETTAZIONE, RICICLAGGIO E AUTORICICLAGGIO

9.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Attività necessarie a prevenire o dirimere una controversia con soggetti terzi – accordi transattivi.
2) Gestione delle operazioni per cassa e dei rimborsi spese al personale.
3) Gestione degli acquisti di beni, servizi, consulenze e prestazioni professionali.
4) Gestione dell'utenza e degli incassi per cassa.
5) Calcolo delle imposte e predisposizione delle dichiarazioni fiscali.
6) Gestione degli investimenti e delle transazioni finanziarie.
7) Emissione di ordini di acquisto, stipulazione di accordi, contratti.

9.2 Reati potenziali

i. Ricettazione (art. 648 c.p.),

ii. Riciclaggio (art. 648 bis c.p.),

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

iv. Autoriciclaggio (art. 648 ter.1 c.p.).

9.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

a) Il reato di ricettazione potrebbe astrattamente realizzarsi laddove vengano conclusi con fornitori contratti di acquisto di materiali, beni o prodotti di provenienza illecita, ad es. frutto di furto o di appropriazione indebita.

b) Il reato di riciclaggio potrebbe astrattamente realizzarsi concludendo transazioni monetarie con clienti con corrispettivi di provenienza illecita.

c) Il reato di autoriciclaggio potrebbe astrattamente realizzarsi laddove la liquidità di proprietà della società, riveniente da reato, ad es. attraverso l'elaborazione di una dichiarazione dei redditi infedele, venga successivamente impiegata in una serie di investimenti finanziari, con modalità tali da occultarne la provenienza delittuosa.

9.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Attività necessarie a prevenire o dirimere una controversia con soggetti terzi – stipulazione di accordi transattivi.	PT 02 – "Contenzioso"
Gestione delle operazioni per cassa e dei rimborsi spese al personale.	PT 05 – "Pagamenti per cassa e rimborsi spese al personale"
Gestione degli acquisti di beni, servizi, consulenze e prestazioni professionali.	PT 08 – "Acquisti"

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione della logistica in entrata e del magazzino.	
Gestione reti ed impianti Gestione controlli	PT 10- "Gestione reti e impianti"
Gestione della tesoreria, gestione dei pagamenti e degli incassi. Gestione dei rapporti con gli istituti di credito e gli intermediari finanziari. Gestione delle transazioni finanziarie, dei pagamenti e degli incassi	PT 09 – "Gestione utenza" PT 12 – "Risorse finanziarie"
Redazione e tenuta delle evidenze economico-patrimoniali relative all'attività / produzione economica tipica e in particolare l'elaborazione e la fornitura dei dati relativi alla produzione tipica industriale. Calcolo delle imposte e predisposizione delle dichiarazioni fiscali.	PT 11 – "Bilancio e dichiarazioni fiscali"
Emissione di ordini, stipulazione di accordi, contratti	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

10 INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

10.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Gestione dei procedimenti penali.

10.2 Reati potenziali

i. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.).

10.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

Il reato potrebbe astrattamente realizzarsi laddove, a fronte di un procedimento giudiziario che veda la Società o propri esponenti in qualità di imputati (ad es. a seguito di un grave infortunio) o come parte lesa (ad es. in un contenzioso con un cliente o un fornitore o un dipendente), taluno induca un proprio subalterno, approfittando della propria posizione gerarchica, a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

10.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione dei procedimenti penali.	PT 02 – "Contenzioso"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

11 REATI AMBIENTALI

11.1 Attività a rischio

In considerazione dell'attività svolta, sono state individuate le seguenti Aree a Rischio Reato:

1) Gestione delle prescrizioni e degli adempimenti legali e normativi.
2) Gestione dei rifiuti.
3) Gestione degli scarichi idrici
4) Elaborazione e tenuta della documentazione, dei registri obbligatori, dei formulari, delle dichiarazioni e delle registrazioni di natura ambientale.
5) Gestione delle emergenze ambientali.
6) Emissione di ordini, stipulazione di accordi e di contratti con soggetti esterni coinvolti nella gestione delle problematiche ambientali – identificazione, raccolta, trasporto, recupero, smaltimento di rifiuti, adempimenti documentali in materia di rifiuti, supporto nella predisposizione delle pratiche autorizzative, controllo dei parametri o dei valori delle sostanze presenti negli scarichi, nelle emissioni, nei rifiuti.
7) Utilizzo di sostanze lesive dell'ozono stratosferico.

11.2 Reati potenziali

I reati potenziali ex D. Lgs. n. 231/01 in materia ambientale sono inclusi in:

- codice penale;
- Lgs. n. 152 del 2006 (cosiddetto Testo Unico sull'Ambiente);
- L. n. 150 del 1992 (Legge di applicazione in Italia della Convenzione sul commercio internazionale di Animali e Vegetali in via di estinzione, c.d. CITES);
- L. n. 549 del 1993 (Legge sulla tutela dell'ozono stratosferico).

11.3 Reati in materia di ambiente contenuti nel codice penale

i. Inquinamento ambientale (art. 452 bis c.p.)
ii. Disastro ambientale (art. 452 quater c.p.)
iii. Delitti colposi contro l'ambiente (art. 452 quinquies c.p.)

iv. Circostanze aggravanti (art. 452 octies c.p.)

11.4 Reati in materia di ambiente contenuti nel D. Lgs. n. 152/2006 (T.U. Ambiente)

v. Art. 137 Scarico di acque

[comma 2] Effettuazione di scarichi di acque reflue industriali senza autorizzazione oppure dopo che l'autorizzazione sia stata sospesa o revocata quando gli scarichi contengono le sostanze pericolose individuate nelle tabelle 5 e 3/A dell'All. 5 del decreto (ad es. Arsenico, Cadmio, Cromo, Mercurio,);

[comma 3] Scarico di acque reflue industriali contenenti le sostanze pericolose (individuate nelle tabelle 5 e 3/A dell'All. 5 del decreto) senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente;

[comma 5] Superamento, nell'effettuazione di uno scarico di acque reflue industriali contenenti le sostanze pericolose (succitate), dei valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'All. 5 del decreto oppure dei limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente;

[comma 11] Inosservanza dei divieti di scarico al suolo e dei divieti di scarichi nel sottosuolo e nelle acque sotterranee di cui agli art. 103 e 104 del Decreto.

vi. Art. 256 Rifiuti

[*comma 1, lett. a*] Attività di raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti svolta in mancanza della prescritta autorizzazione (artt. da 208 a 216 del decreto);

[*comma 1, lett. b*] medesima fattispecie di cui alla lett. a), riferita però ai rifiuti pericolosi;

[*comma 3 primo periodo*] Realizzazione o gestione di una discarica non autorizzata;

[*comma 3 primo periodo*] Realizzazione o gestione di una discarica non autorizzata destinata, anche solo in parte, allo smaltimento di rifiuti pericolosi;

[comma 5] Attività non consentita di miscelazione dei rifiuti in violazione del divieto di cui all'art. 187 del Decreto;

[*comma 6*] Deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi in violazione dell'art. 227 del decreto.

vii. Art. 257 Bonifica dei siti

[*comma 1*] Inquinamento del suolo, del sottosuolo, delle acque superficiali o sotterranee con superamento delle concentrazioni soglia di rischio (in mancanza di bonifica in conformità ai dettami del Decreto);

[*comma 2*] medesima fattispecie di cui al co. 1, ma con inquinamento provocato da sostanze pericolose.

viii. Art. 258 - Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari

[*comma 4*] False indicazioni, nella predisposizione di un certificato di analisi di rifiuti, sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, e utilizzo di certificato falso durante il trasporto.

ix. Art. 259 Traffico illecito di rifiuti

[*comma 1*] Chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del regolamento stesso è punito con la pena dell'ammenda da 1.550 euro a 26.000 euro e con l'arresto fino a due anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi

x. Art. 260 Attività organizzate

[*comma 1*] Attività organizzata per il traffico illecito di rifiuti;

[*comma 2*] Attività organizzata per il traffico illecito di rifiuti ad alta radioattività.

xi. Art. 260-bis SISTRI

[*comma 6*] predisporre un certificato di analisi dei rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, in cui sono fornite false indicazioni sulla natura composizione e caratteristiche chimico-fisiche dei rifiuti;

[*comma 7, secondo periodo*] omissione, nel trasporto di rifiuti pericolosi, di accompagnamento degli stessi con copia cartacea della scheda SISTRI – *area movimentazione*;

[*comma 7, terzo periodo*] utilizzo, durante il trasporto, di un certificato di analisi di rifiuti contenente false indicazioni;

[*comma 8, primo periodo*] accompagnamento del trasporto di rifiuti con copia cartacea della scheda "*SISTRI – area movimentazione*" fraudolentemente alterata;

[*comma 8, secondo periodo*] medesima fattispecie di cui al primo periodo ma con riferimento a rifiuti pericolosi.

xii. Art. 279 (Immissioni in atmosfera)

[*comma 5*] Superamento, nell'esercizio di uno stabilimento, dei valori limite di emissione.

11.5 Reati ambientali rilevanti ex D. Lgs. n. 231/01 contenuti nella L. n. 549 del 1993 (Legge sulla tutela dell'ozono stratosferico e dell'ambiente)

xiii. Art. 3

[*comma 6*] Produzione, consumo, importazione o commercializzazione della sostanza lesiva di cui alla tabella A della stessa legge (idrocarburi idrogenati contenenti fluoro e cloro).

11.6 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

a) Una non corretta attribuzione del codice CER ai rifiuti prodotti può comportare un conferimento rifiuto a terzi che non sono abilitati a riceverlo, qualora nell'abilitazione del destinatario figuri il codice erroneamente attribuito, ma non quello che correttamente si sarebbe dovuto attribuire. Se, poi, per effetto dell'errore nell'attribuzione del codice, si sbaglia anche nella classificazione qualificando non pericoloso un rifiuto che invece lo è (il codice erroneamente attribuito non è contrassegnato da asterisco, mentre lo è quello che si sarebbe dovuto attribuire) L'evento è possibile nella gestione, ad esempio, dei toner utilizzati presso gli uffici. I reati configurabili potrebbero essere in via astratta art. 256 co 1 lett. a) (rifiuti non pericolosi) e lett. b) (rifiuti pericolosi) del TU ambientale

b) Lo scenario già descritto, (errata caratterizzazione dei rifiuti con codice CER non corretto) espone al rischio di miscelazione di rifiuti, sanzionato all'art. 256 comma 5

c) Una errata (incompleta o inesatta) compilazione del formulario profila il reato previsto dall'art. 258 del TU ambientale

d) il reato di inquinamento potrebbe astrattamente realizzarsi laddove un problema tecnologico agli impianti, dovuto ad esempio ad una carente manutenzione, o un'operazione non correttamente effettuata rilasci nell'ambiente (nelle acque, nell'aria, nel suolo) sostanze (fuoriuscita di liquidi, gas o dispersione di particelle

solide) in grado di compromettere o deteriorare in modo significativo e misurabile il contesto ambientale. Ad esempio, la semplice caduta e rottura di una cisterna contenente olio in prossimità di un punto di scolo, se non prontamente gestita, può comportare la diffusione dell'olio in adiacenti corsi d'acqua

11.7 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione delle prescrizioni e degli adempimenti legali e normativi. Gestione dei rifiuti. Elaborazione e tenuta della documentazione, dei registri obbligatori, dei formulari, delle dichiarazioni e delle registrazioni. Controllo della dispersione di sostanze lesive dell'ozono stratosferico. Gestione delle emergenze ambientali.	PT 17 – "Tutela dell'Ambiente"
Emissione di ordini, stipulazione di accordi, contratti.	PT 18 – "Protocollo contrattuale generale"

Per prendere visione dei protocolli sopra richiamati si rinvia al capitolo "Protocolli di prevenzione e di gestione".

12 IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

12.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Selezione e assunzione di personale.
2) Gestione e amministrazione del personale.

12.2 Reati potenziali

i. Art. 22, commi 12 e 12 bis, Decreto Legislativo 25 luglio 1998, n. 286 (Lavoro subordinato a tempo determinato e indeterminato).

12.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

Il reato potrebbe astrattamente realizzarsi laddove si assumessero cittadini senza permesso di soggiorno o con lo stesso scaduto.

12.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Selezione e assunzione di personale. Gestione e amministrazione del personale.	PT 07 – "Selezione, assunzione e gestione del personale"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".

13 REATI TRIBUTARI

13.1 Attività a rischio

In considerazione della peculiarità delle attività aziendali svolte, sono state individuate le seguenti Aree a Rischio Reato:

1) Calcolo delle imposte e liquidazione dei relativi importi.
2) Predisposizione delle dichiarazioni fiscali.
3) Esecuzione di operazioni societarie.
4) Gestione della tesoreria.

Aree a Rischio strumentali alla consumazione del reato:

5) Gestione dell'utenza, emissione delle fatture, gestione dei crediti.
6) Gestione dei contratti e degli ordini di acquisto.
7) Redazione e tenuta delle evidenze economico–patrimoniali relative all'attività/produzione economica tipica.
8) Accesso, gestione e aggiornamento delle registrazioni contabili tramite il sistema gestionale aziendale.
9) Redazione e tenuta delle scritture contabili.
10) Gestione dei rapporti con gli istituti di credito e gli intermediari finanziari.
11) Gestione del sistema informativo aziendale.

13.2 Reati potenziali

i. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2, D. Lgs. 10 marzo 2000, n. 74),
ii. Dichiarazione fraudolenta mediante altri artifici (Art. 3, D. Lgs. 10 marzo 2000, n. 74),
iii. Dichiarazione infedele (Art. 4 D. Lgs. 10 marzo 2000, n. 74),
iv. Omessa dichiarazione (Art. 5 D. Lgs. 10 marzo 2000, n. 74),
v. Emissione di fatture o altri documenti per operazioni inesistenti (Art. 8, D. Lgs. 10 marzo 2000, n. 74),
vi. Occultamento o distruzione di documenti contabili (Art. 10, D. Lgs. 10 marzo

2000, n. 74),

vii. Indebita compensazione (Art. 10-quater D. Lgs. 10 marzo 2000, n. 74),

viii. Sottrazione fraudolenta al pagamento di imposte (Art. 11, D. Lgs. 10 marzo 2000, n. 74).

13.3 Esemplificazione delle modalità attraverso le quali potrebbero essere commessi i reati

a) Il reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti potrebbe astrattamente realizzarsi qualora la Società:

- utilizzi i documenti fiscali rilasciati da imprese fittizie dette anche "società di comodo", create al solo fine di consentire ad altri operatori economici di evadere le imposte, attraverso la giustificazione contabile delle cessioni di beni o prestazioni di servizi effettuate da ulteriori imprese, realmente operative, che vengono celate al Fisco.
- Faccia formalmente assumere personale a "società di comodo", che emettono fatture per prestazioni di servizio "gonfiate" nei confronti della Società realizzando, di conseguenza, un'indebita deduzione di costi per la parte eccedente al costo effettivo del personale.

b) Il reato di dichiarazione fraudolenta mediante altri artifici potrebbe astrattamente realizzarsi qualora la Società:

- utilizzi documenti contraffatti o alterati, diversi dalle fatture o altri documenti per operazioni inesistenti oggetto di falsità sia ideologica che materiale, quali, ad esempio:
  - l'imputazione di spese relative a investimenti inesistenti sorretta da predisposizione di contratti ideologicamente falsi;
  - contratti simulati (ovvero rogiti notarili attestanti compravendite immobiliari) con indicazione di un prezzo di vendita molto inferiore al reale;
- intesti fittiziamente rapporti finanziari su cui accreditare elementi attivi destinati a non essere contabilizzati;
- emetta titoli di credito senza indicazione del beneficiario al fine di occultarne i pagamenti.

c) Il reato di occultamento o distruzione di documenti contabili potrebbe

astrattamente realizzarsi qualora la Società:

- impedisca il rinvenimento delle scritture e dei documenti fiscali nel luogo dichiarato ai sensi di legge e tale omissione si riveli preordinata ad impedire l'analisi documentale da parte dell'Amministrazione finanziaria;
- conservi la contabilità, archiviata elettronicamente e regolarmente istituita ma, al fine di evadere le imposte e ostacolare l'accertamento, in luoghi diversi da quelli previsti ai sensi di legge;
- venga inibito l'accesso all'Amministrazione finanziaria alla documentazione contabile ed extra-contabile, la cui tenuta sia normativamente prevista, archiviata in un server ubicato in uno Stato estero, anche quando siano esistenti strumenti di cooperazione amministrativa con lo Stato estero presso cui siano allocati i server di archiviazione.

d) La condotta tipica del reato di sottrazione fraudolenta al pagamento di imposte è integrata da qualsiasi atto o fatto fraudolento, intenzionalmente teso a ridurre la capacità patrimoniale della società contribuente in modo da vanificare o, comunque, ostacolare un'eventuale procedura esecutiva. Il reato potrebbe astrattamente realizzarsi qualora la Società:

- simuli la messa in liquidazione e la cessazione della stessa, proseguendo, contestualmente alla cessazione, la medesima attività d'impresa, con gli stessi dipendenti e negli stessi locali della cessata, per il tramite di un'altra società;
- metta in atto un'operazione di riorganizzazione aziendale, attraverso la quale la Società, divenuta responsabile verso il Fisco per il pagamento dei tributi, venga svuotata di ogni attività a favore di altre società riconducibili alla medesima compagine societaria, lasciando residuare in capo alla prima, quale unico rapporto giuridico pendente, il debito fiscale.

13.4 Prevenzione del rischio nello svolgimento delle attività sensibili

Al fine di mitigare il pericolo insito nelle attività a rischio così come sopra richiamate, la Società ha adottato i protocolli indicati nella seguente tabella.

ATTIVITA' SENSIBILE	PROTOCOLLO DI RIFERIMENTO
Gestione dei contratti e degli ordini di acquisto	PT 08 – "Acquisti"
Gestione utente Gestione misure	PT 09 – "Gestione utenza"
Gestione reti ed impianti Gestione controlli	PT 10 – "Gestione reti e impianti"
Redazione e tenuta delle evidenze economico–patrimoniali relative all'attività/produzione economica tipica. Accesso, gestione e aggiornamento delle registrazioni contabili tramite il sistema gestionale aziendale. Redazione e tenuta delle scritture contabili.	PT 11 – "Bilancio e dichiarazioni fiscali"
Gestione dei rapporti con gli istituti di credito e gli intermediari finanziari. Gestione della tesoreria.	PT 12 – "Risorse finanziarie"
Esecuzione di operazioni societarie.	PT 14 – "Operazioni relative al capitale sociale e adempimenti societari"
Gestione del sistema informativo aziendale.	PT 15 – "Sistema informativo"

Per prendere visione dei protocolli sopra richiamati si rinvia alla successiva Sezione "Protocolli di prevenzione e di gestione".